Recht doen aan privacyverklaringen

Verhelst, E.W.

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

RECHT DOEN AAN PRIVACYVERKLARINGEN

EEN JURIDISCHE ANALYSE VAN PRIVACYVERKLARINGEN OP INTERNET

Eric W. Verhelst

Het leven is een pelgrimstocht

RECHT DOEN AAN PRIVACYVERKLARINGEN

EEN JURIDISCHE ANALYSE VAN PRIVACYVERKLARINGEN OP INTERNET

Proefschrift ter verkrijging van de graad van doctor aan Tilburg University op gezag van de rector magnificus, prof. dr. Ph. Eijlander, in het openbaar te verdedigen ten overstaan van een door het college voor promoties aangewezen commissie in zaal DZ 1 van de Universiteit

op vrijdag 11 mei 2012 om 14.15 uur

door

Eric Willem Verhelst
geboren op 14 oktober 1968 te Rijswijk (ZH)

Promotor:

Prof. mr. J.E.J. Prins

Promotiecommissie:

Prof. mr. J.M.A. Berkvens
Mr. dr. C.M.K.C. Cuijpers
Prof. mr. drs. C. Stuurman
Prof. mr. G-J. Zwenne

Woord vooraf

Dit proefschrift zou niet tot stand zijn gekomen zonder de hulp en onvoorwaardelijke steun van anderen. Mijn grote dank gaat uit naar prof. mr. J.E.J. Prins voor haar inspiratie, suggesties, tijd en bemoedigende woorden. Ik ben trots en vereerd dat zij *mijn* promotor is. Tevens wil ik mijn dank uitspreken aan de promotiecommissie, prof. mr. J.M.A. Berkvens, mr. dr. C.M.K.C. Cuijpers, prof. mr. drs. C. Stuurman & prof. mr. G-J. Zwenne, voor het nauwgezet hebben gelezen van het manuscript en het waardevolle commentaar. Tegen mijn familie, in het bijzonder Magda, Femke, Mees & Ties, en vrienden wil ik zeggen: “Ik hou van jullie”. Deze dissertatie draag ik op aan mijn vader. Het was hem slechts gegeven mijn ‘carrière’ op de basisschool te mogen meemaken. Mijn inschatting is dat hij met gepaste trots dit promotietraject zou hebben aanschouwd. *Het is zoals het is*.

Eric Verhelst
Tilburg, mei 2012

Inhoudsopgave

Lijst van afkortingen

aant.	aantekening
AG	Advocaat-Generaal
BNB	Beslissingen in belastingzaken / Nederlandse belastingrechtspraak
Bude	Besluit universele dienstverlening en eindgebruikersbelangen
B.U. J. SCI. & TECH. L.	Boston University Journal of Science & Technology Law
BW	Burgerlijk Wetboek
Cbp	College bescherming persoonsgegevens
diss.	dissertatie
EC	Europese Commissie
EHRM	Europees Hof voor de Rechten van de Mens
EG	Europese Gemeenschap
et al.	et alii
EU	Europese Unie
e.v.	en volgende
EVRM	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
FG	Functionaris voor de Gegevensbescherming
FTC	Federal Trade Commission
GW	Grondwet
HR	Hoge Raad
HvJEG	Hof van Justitie van de Europese Gemeenschappen
jo.	juncto
JOL	Jurisprudentie On-line
JOR	Jurisprudentie Onderneming & Recht
MvT	Memorie van Toelichting
NJ	Nederlandse Jurisprudentie
nr.	nummer
n.s.	niet significant
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
o.g.v.	op grond van
p.	pagina
para.	paragraaf
PbEG	Publicatieblad van de Europese Gemeenschappen
P&I	Privacy & Informatie

Privacyrichtlijn	Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens
RF	Rechtspraak Financieel recht
RO	Wet op de rechterlijke organisatie
r.o.	rechtsoverweging
RvdW	Rechtspraak van de Week
Stb.	Staatsblad
TW	Telecommunicatiewet
VwEU	Verdrag betreffende de werking van de Europese Unie
Wbp	Wet bescherming persoonsgegevens
WPNR	Weekblad voor Privaatrecht, Notariaat en Registratie
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Hoofdstuk 1 | Inleiding

1.1 Inleiding

In februari 2012 kondigt het bedrijf Google Inc. aan dat het zijn 60 online privacyverklaringen zal consolideren naar één privacyverklaring.[1] De tot op heden separate privacyverklaringen zien op verschillende online diensten die Google biedt, zoals de zoekmachine, Youtube, Gmail, Picasa, Google Books, Google Desktop en Blog Search. Het voornemen lijkt vanuit het oogpunt van transparantie een nobel streven. Het staartje zit in de mededeling van Google dat het de persoonsgegevens, die via zijn verschillende diensten wordt verkregen, ook zal consolideren. Daarmee krijgt Google inzicht in het persoonlijk wel en wee van duizenden gebruikers.[2]

De plannen van Google maken onder meer duidelijk dat door de uitvoering van enkele technische handelingen de informationele privacy van miljoenen individuen in het geding is.[3] De Europese Commissie wees in dit verband al eerder op de consequenties van nieuwe technologische en maatschappelijke ontwikkelingen. “Met de technologie van vandaag kunnen personen gemakkelijk informatie uitwisselen over hun gedragingen en voorkeuren en die informatie op een nooit geziene schaal publiek en wereldwijd toegankelijk maken”.[4] De Commissie noemt als voorbeeld het gebruik van sociale netwerksites. Ook doelt de Commissie op het fenomeen cloud computing, waarmee het risico wordt vergroot dat “personen geen controle meer hebben over hun potentieel gevoelige informatie wanneer zij gegevens opslaan met behulp van programma's die gehost worden op hardware van iemand anders”.[5] Ook cookies (software die al dan niet heimelijk persoonsgegevens verzamelt), zijn niet meer weg te denken uit ons dagelijks digitale leven. Het gebruik van cookies leek bij de introductie wellicht onschuldig. Heden ten dage is het realiteit dat een informatiegigant als Facebook, met behulp van cookies, op niet-transparante wijze zelfs bij personen die geen Facebook hebben persoonsgegevens verzamelt.[6] Het huidige debat

---

1 Alma Whitten, Director of Privacy, Product and Engineering. http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.

2 De Groep Gegevensbescherming Artikel 29 heeft in reactie Google verzocht het voornemen uit te stellen totdat alle gevolgen zijn te overzien. Groep Gegevensbescherming Artikel 29, 2 February 2012, Ref. Ares(2012)123126-02/02/2012.

3 Naar de mening van Blok is het algemeen aanvaard om informationele privacy te omschrijven als ‘regie over de eigen persoonsgegevens’. Blok, p. 123. Volgens Dommering ziet informationele privacy op de rechten van het individu om de opslag van zijn persoonsgegevens te verhinderen, te beperken of te veranderen en ziet het ook op de verplichtingen en beperkingen die gelden voor de personen en instellingen die deze persoonsgegevens opslaan. Dommering 2000, p. 50 e.v.

4 COM (2010) 609 definitief, p. 2.

5 COM (2010) 609 definitief, p. 2.

6 Zie Roosendaal.

rondom dit en ander gebruik van cookies valt echter in het niet bij de consequenties die ons te wachten staan wanneer de zogenaamde ambient intelligence-visie werkelijkheid wordt. Deze visie voorspelt een wereld waarin technologie een totale, permanente, en allesomvattende aanwezigheid in onze dagelijks levens wordt.[7] De technologie is adaptief, hetgeen tot gevolg heeft dat de technologie ons gedrag over langere periodes zal volgen, onze gedragingen zal interpreteren en evalueren en vervolgens zal samenvoegen tot een profiel, zodat de technologie haar diensten in een volgende, vergelijkbare situatie (nog) beter kan afstemmen op de behoeften van de gebruiker.[8] "Tot slot is het van belang, zo stelt de ambient intelligence-visie, dat de technologie de gebruiker niet alleen actief van context- en persoonsgebonden informatie zal gaan voorzien, maar zelfs proactief".[9] De gebruiker hoeft daarmee niet meer actief op zoek naar informatie, maar wordt hem, contextgebonden en gepersonaliseerd, als vanzelf door de technologie voorgeschoteld. Naar de verwachting van Stuurman zal ambient intelligence zich qua maatschappelijke impact kunnen meten met ontwikkelingen als de opkomst van mobiele communicatie en het Internet.[10] Vanuit juridisch perspectief oogt ambient intelligence als een sprookje vanwege de vele uitdagende vragen, aldus Stuurman.[11] Vanuit het perspectief van het individu in relatie tot de bescherming van zijn persoonsgegevens wordt het waarschijnlijk echter een nachtmerrie.[12]

Purtova signaleert twee trends met betrekking tot het verwerken van persoonsgegevens. "The first is the constantly growing thirst for information, both in public and private sector". "The second trend is the growing capacity of technology to accommodate the desire for more information, personalisation and better communication".[13] Vervolgens onderkent zij een aantal zorgen (*concerns*) met betrekking tot de verwerking van persoonsgegevens in relatie tot de hiervoor geschetste technologische en maatschappelijke ontwikkelingen.[14] Een daarvan betreft het gebrek aan transparantie en accountability in de keten van gegevensverwerkingen.[15] Kijkend vanuit het perspectief van het individu, is het, gezien de geschetste ontwikkelingen, vrijwel niet mogelijk te bepalen door wie, waar en welke persoonsgegevens van hem worden verwerkt. De Europese Commissie expliciteert daarom dat het van wezenlijk belang is dat individuen goed, duidelijk en op een transparante wijze worden geïnformeerd over hoe en door wie hun gegevens worden verzameld en verwerkt, voor welke doeleinden, gedurende welke periode en in hoeverre zij het recht hebben hun

7 Van den Berg, p. 268.
8 Van den Berg, p. 268.
9 Van den Berg, p. 269.
10 Stuurman, p. 262.
11 Stuurman, p. 262.
12 Zie in dit kader Hildebrandt, p. 278 e.v.
13 Purtova, p. 39.
14 Purtova, p. 40 e.v.
15 Purtova, p. 48.

gegevens in te zien, te corrigeren of te wissen.[16] De Commissie is dan ook van mening dat transparantie een basisvoorwaarde is, willen individuen controle kunnen uitoefenen over hun eigen gegevens en zich van een effectieve bescherming van hun persoonsgegevens kunnen verzekeren.[17] Tevens benadrukt de Europese Commissie het belang van accountability, en stelt dat moet worden nagegaan hoe het best kan worden verzekerd dat de verantwoordelijke *de facto* beleid voert en mechanismen instelt ter naleving van de regels inzake gegevensbescherming.[18]

In Nederland zijn de regels met betrekking tot het verwerken van persoonsgegevens in het bijzonder vastgelegd in de Wet bescherming persoonsgegevens (Wbp). De Wbp is in 2001 in werking getreden, en vormt de implementatie van de Privacyrichtlijn uit 1995.[19] Een belangrijke bepaling in zowel de Richtlijn als daarom ook de Wbp is die betreffende de transparantie over de gegevensverwerking. De Wbp kent, conform de artikelen 33 en 34 Wbp, een informatieplicht die de verantwoordelijke in acht dient te nemen indien er sprake is van verwerking van persoonsgegevens. Voornoemde artikelen vormen zoals gezegd een uitwerking van het – niet als zodanig in de Wbp geëxpliciteerde – transparantiebeginsel, maar zeker ook het in artikel 6 Wbp neergelegde 'fair processing' beginsel. Op grond van de informatieplicht dient de verantwoordelijke zijn identiteit bekend te maken, alsmede de verwerkingsdoeleinden waarvoor de gegevens bestemd zijn. Tevens dient de verantwoordelijke nadere informatie te verstrekken indien dat noodzakelijk is gelet op (i) de aard van de gegevens en/of (ii) de omstandigheden waaronder de gegevens worden verkregen en/of (iii) het gebruik dat van de gegevens wordt gemaakt. De wetgever heeft niet geregeld op welke wijze (mondeling, schriftelijk of elektronisch) of in welke vorm (bijvoorbeeld per e-mail of SMS) de verplichte informatie dient te worden verstrekt. In de praktijk blijkt de online privacyverklaring een populair instrument voor de verantwoordelijke om via zijn website te trachten te voldoen aan de informatieplicht uit de Wbp. Het gebruik van dit instrument roept diverse vragen op. Vragen die zowel de Wbp zelf betreffen als de privaatrechtelijke context waarbinnen de afspraken over de verwerking van persoonsgegevens veelal vorm krijgen. Kan bijvoorbeeld een betrokkene bepaalde rechten ontlenen aan de informatie die door de verantwoordelijke via de privacyverklaring wordt verstrekt, en zo ja, op welke wijze kan de betrokkene dit recht effectueren? Kunnen de verantwoordelijke en de betrokkene gezamenlijk in een privacyverklaring afspraken maken

16 COM (2010) 609 definitief, p. 6.

17 COM (2010) 609 definitief, p. 6.

18 COM (2010) 609 definitief, p. 13. In dit onderzoek zal blijken dat ook de Groep Gegevensbescherming Artikel 29 en overige adviescommissies de noodzaak van meer transparantie en accountability in relatie tot de verwerking van persoonsgegevens benadrukken.

19 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), Stb. 2000, 302; Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. PbEG Nr. L 281/31.

over de wijze waarop de persoonsgegevens worden verwerkt? Ofwel, kan een privacyverklaring via de band van het privaatrecht worden gekwalificeerd als een overeenkomst, en zo ja, wordt de inhoud van zo'n privacyovereenkomst mogelijk beperkt door de Wbp? Is de privacyverklaring mogelijk te kwalificeren als elektronische algemene voorwaarden? De Europese Commissie benadrukt in recente plannen en initiatieven het belang van transparantie en accountability, maar aan welke voorwaarden dient concreet een privacyverklaring te voldoen wil het daadwerkelijk betekenis krijgen voor deze belangen? Dient er wellicht door bepaalde actoren, te denken valt aan de wetgever, toezichthouder of de sector zelf, via nadere regelgeving op de vorm, inhoud en het gebruik van de privacyverklaring gestuurd te worden opdat transparante privacyverklaringen worden ontwikkeld en gebruikt?

Gegeven zowel de toenemende populariteit van het gebruik van privacyverklaringen door aanbieders van webdiensten als de nadruk die de Europese wetgever meer recent legt op het belang van transparantie en accountability, is het opvallend dat er niet tot nauwelijks wetenschappelijk onderzoek voorhanden is naar de juridische context waarbinnen de privacyverklaring vorm, inhoud en rechtskracht verkrijgt. Ook ontbreekt nader onderzoek naar de relatie tussen enerzijds het gebruik in de praktijk van de privacyverklaring en anderzijds de al dan niet noodzaak om op dit gebruik te sturen via nadere regulering. Interessant daarbij is dat in de Verenigde Staten de afgelopen jaren diverse onderzoeken zijn uitgevoerd naar het gebruik van privacyverklaringen en de wenselijkheid om hier – via standaardisatie – op te sturen. Gegeven het toenemende belang van de privacyverklaring als instrument om de in de Wbp neergelegde transparantieplicht invulling te geven in combinatie met het ontbreken van een bredere wetenschappelijke duiding van dit instrument, richt deze dissertatie zich op zowel de juridische kwalificatie van de privacyverklaring, het gebruik van deze verklaring in de praktijk alsmede de mogelijkheden en wenselijkheid om op het gebruik, vorm en de inhoud van de privacyverklaring te sturen via wetgeving dan wel (zelf)regulering. Een dergelijke analyse is mede van belang nu de Europese Commissie begin 2012 in het voorstel voor een aanpassing van Richtlijn 95/46 in lijkt te zetten op mogelijke sturing vanuit de Commissie op de invulling van de transparantieplicht.

1.2 Probleemstelling

Gegeven de hiervoor gepresenteerde ambitie staan de volgende onderzoeksvragen in dit onderzoek centraal:

1. Wat is de juridische status van een online privacyverklaring?
2. Hoe krijgt de online privacyverklaring in de praktijk vorm en inhoud?

3. In hoeverre, en door welke actor, dient nader op de vorm, inhoud en het gebruik van een online privacyverklaring te worden gestuurd, mede met het oog op ontwikkelingen op EU-niveau?

1.3 Opzet van het onderzoek

De eerste onderzoeksvraag wordt beantwoord aan de hand van de hoofdstukken 2 en 3. Daartoe start hoofdstuk 2 met een verkenning aan de hand van de literatuur, van de in de Wbp opgenomen informatieplicht en wordt getracht de privacyverklaring als instrument te kwalificeren vanuit het perspectief van de Wbp.
Vervolgens wordt in hoofdstuk 3 de privacyverklaring vanuit een privaatrechtelijk perspectief nader onder de loep genomen. De privacyverklaring kan immers breder worden toegepast dan uitsluitend als instrument ter concretisering van de informatieplicht uit de Wbp. De verantwoordelijke en de betrokkene kunnen afspraken maken die weliswaar zien op of gerelateerd zijn aan de verwerking van persoonsgegevens, maar die op grond van de Wbp niet hoeven te worden opgenomen in een privacyverklaring. Kijkend vanuit het perspectief van het Burgerlijk Wetboek (BW) zou een privacyverklaring mogelijk zijn te kwalificeren als een overeenkomst tussen de verantwoordelijke en de betrokkene. Allereerst wordt in hoofdstuk 3 onderzocht of de verantwoordelijke en de betrokkene een overeenkomst kunnen sluiten met betrekking tot de verwerking van persoonsgegevens, en zo ja, of en in hoeverre zij daarin worden beperkt door de Wbp. Tevens zal aandacht worden besteed aan de wijze waarop een privacyovereenkomst op elektronische wijze tot stand kan komen. Vervolgens worden de (rechts)maatregelen besproken die de betrokkene kan treffen indien de verantwoordelijke zijn verplichtingen uit de privacyovereenkomst niet nakomt. Ook wordt bezien in hoeverre de betrokkene in dat geval schadevergoeding kan vorderen. Tot slot zal in hoofdstuk 3 worden onderzocht of een privacyverklaring kan worden gekwalificeerd als elektronische algemene voorwaarden.

Hoofdstuk 4 beoogt de tweede onderzoeksvraag te beantwoorden en doet daartoe verslag van een empirisch onderzoek naar privacyverklaringen onder 257 online winkels in de marktsegmenten Verzekeringen, Reizen en Kleding. Het onderzoek brengt het feitelijk gebruik van de privacyverklaring in enkele sectoren nader in beeld. Aan de hand van het verkregen materiaal wordt onderzocht of sturing door brancheorganisaties op het gebruik van privacyverklaringen effect lijkt te sorteren.

De derde onderzoeksvraag komt aan de orde in de hoofdstukken 5 en 6. Hoofdstuk 5 blikt allereerst terug op de conclusies uit de voorgaande hoofdstukken, en destilleert daaruit knelpunten wat betreft het huidige gebruik van privacyverklaringen. Voorts wordt in dit hoofdstuk gekeken naar relevante ontwikkelingen op EU-niveau. Tevens zal, redenerend

vanuit transparantie en accountability, worden gekeken naar de wenselijke vorm en inhoud van een privacyverklaring. Hierbij wordt in ieder geval gerefereerd aan onderzoek in de Verenigde Staten naar sturing op privacyverklaringen.
Aan de hand van de conclusies uit de verschillende voorgaande hoofdstukken wordt in hoofdstuk 6 de stap gezet naar de vraag of nadere sturing moet plaatsvinden met betrekking tot de ontwikkeling van gestandaardiseerde privacyverklaringen, en vervolgens het gebruik daarvan. Hierbij liggen opties via overheids- dan wel zelfregulering als mogelijke scenario's voor. Kijkend naar een te prefereren keuze voor zelfregulering, wordt in hoofdstuk 6 aandacht besteed aan enkele kenmerken en consequenties van sturing via zelfregulering. Voorts wordt onderzocht welke rol zelfregulering kan vervullen bij een nadere uitwerking van de informatieplicht, via het op brancheniveau ontwikkelen van gestandaardiseerde sectorale privacyverklaringen. Tevens bevat dit hoofdstuk aanbevelingen, en wordt het ambitieniveau beschreven dat ten aanzien van gestandaardiseerde sectorale privacyverklaringen nagestreefd zou moeten worden.

Tot slot wordt het onderzoek in hoofdstuk 7 afgesloten aan de hand van conclusies.

1.4 Belang van het onderzoek

Hiervoor is al kort gerefereerd aan het belang van het onderhavige onderzoek. In aanvulling hierop zijn de volgende overwegingen van belang. Zoals beschreven zullen de komende twee hoofdstukken vanuit het perspectief van de Wbp en het BW de juridische status van een privacyverklaring nader proberen te duiden. Een dergelijke duiding is wenselijk – zeker nu de privacyverklaring aan populariteit wint en het belang van transparantie door de wetgever benadrukt wordt – met het oog op meer rechtszekerheid voor zowel de verantwoordelijke als de betrokkene.

Relevant is hier ook de hervorming van de Privacyrichtlijn zoals die op 25 januari 2012 door de Europese Commissie is gepresenteerd.[20] Een van de ambities bij deze hervorming betreft het versterken van het recht van de betrokkene op informatie, zodat deze volledig (beter) begrijpt op welke wijze zijn persoonsgegevens worden verwerkt.[21] Uit het voorstel blijkt dat de Europese Commissie deze doelstelling wil bereiken door explicitering van het transparantie en accountability beginsel, en tevens lijkt te gaan sturen op het ontwikkelen en het gebruik van gestandaardiseerde privacyverklaringen. Dit onderzoek beoogt te verduidelijken of en in hoeverre verantwoordelijken die via hun website producten of diensten exploiteren, hun informatieplicht nakomen met behulp van een privacyverklaring,

20 COM (2012) 11 final.
21 COM (2012) 9 final, p. 6.

en op welke wijze zij via een dergelijke verklaring nader invulling geven aan die informatieplicht. Aan de hand hiervan kan worden bepaald of de huidige privacyverklaringen, wat betreft vorm en inhoud, daadwerkelijk betekenis hebben voor transparantie en accountability. Tevens kan dit onderzoek een bijdrage leveren aan de discussie over het ontwikkelen en het gebruik van gestandaardiseerde privacyverklaringen, alsmede of sturing via overheidsregulering en/of zelfregulering wenselijk is.

Zoals gezegd, ziet dit onderzoek op online privacyverklaringen op websites. Een website is slechts een online kanaal waarmee producten en diensten kunnen worden aangeboden. De technologische ontwikkelingen staan niet stil, hetgeen tot gevolg heeft dat producten en diensten ook op andere wijzen dan via de traditionele variant van een computer aangesloten op het Internet aangeboden kunnen worden. Als voorbeeld kan natuurlijk worden genoemd de zogeheten Apps. Alhoewel dit onderzoek (zeker wat betreft het empirisch deel) beperkt is tot het beschikbaar stellen van de privacyverklaring via webpagina's, bieden de analyse en conclusies zeker aanknopingspunten bij het denken over de wijze waarop betrokkenen geïnformeerd kunnen worden indien andere elektronische kanalen worden gehanteerd.

Dit onderzoek is mede ingegeven vanuit de overtuiging dat er behoefte is aan meer empirisch materiaal over de werking van het recht. Deze overtuiging sluit aan bij de oproep van zowel Vranken als Van Dijck in hun bijdragen van eind 2011 in WPNR tot meer aandacht voor hetgeen feitelijk met het recht gebeurt. Deze oproep past in de recente aandacht voor wat wordt genoemd een nieuwe vorm van rechtsrealisme en 'Empirical Legal Scholarship'.[22] De oproep om in het nieuwe rechtsrealisme meer aandacht te besteden aan wat feitelijk gebeurt (de bottom-up-benadering) uit zich in een meer empirische bestudering van het privaatrecht, aldus Vranken en Van Dijck.[23] "De les van het Amerikaanse rechtsrealisme daarbij is dat wie aansluiting bij de praktijk wil houden, oog moet hebben voor de kennisbehoefte die daar leeft, maar tegelijkertijd iets meer en iets anders moet doen dan wat in de praktijk reeds gebeurt. Dat andere en meerdere kan bijvoorbeeld zitten in ontmaskeren of aanvullen, maar ook in het verklaren van ontwikkelingen in de privaatrechtelijke praktijk".[24] Beide auteurs stellen voorts dat een meer realistische benadering van het privaatrecht tevens kan worden aangeduid als een evidence-based approach. "Empirische inzichten kunnen het bestaande juridische denkkader aanvullen, verfijnen, en bepaalde aannames of veronderstellingen ontkrachten. Ze kunnen echter het juridische denkkader niet vervangen, in ieder geval niet geheel".[25] Het empirisch onderzoek dat in deze dissertatie is uitgevoerd past in deze ontwikkeling en geeft meer specifiek een

22 Vranken & Van Dijck, p. 1124 e.v. Zie in dit kader tevens Vranken 2011 en Van Dijck. Laatstgenoemde spreekt van 'Empirical Legal Studies'.

23 Vranken & Van Dijck, p. 1124.

24 Vranken & Van Dijck, p. 1124.

25 Vranken & Van Dijck, p. 1125.

beeld van het feitelijk gebruik van privacyverklaringen. De resultaten leveren een 'rechtsrealistische' bijdrage aan het denken over privacyverklaringen, en de wijze waarop nader op de vorm, inhoud en het gebruik van een online privacyverklaring kan worden gestuurd.

Tot slot tracht dit onderzoek voor wat betreft het instrument van de privacyverklaring een bijdrage te leveren aan de wens om 'law in the books' ook te duiden vanuit 'law in action'. Met law in action wordt bedoeld dat wettelijke vereisten moeten worden omgezet in daadwerkelijke maatregelen ter bescherming van gegevens.[26] Dit onderzoek maakt duidelijk welke concrete stappen moeten worden genomen opdat gestandaardiseerde sectorale privacyverklaringen worden ontwikkeld en gebruikt.

1.5 Afbakening

Het Internet kenmerkt zich door de mondiale en grenzeloze schaal en is niet aan territoriale grenzen gebonden; de plaats waar actoren en computernetwerken zich bevinden, alsmede de plaats waar persoonsgegevens daadwerkelijk worden verwerkt, hoeven niet meer één te zijn. Voor het internationale recht is dan ook een belangrijke rol weggelegd bij de beantwoording van rechtsvragen die gerelateerd zijn aan het Internet. Dit onderzoek laat zich inspireren door buitenlandse ontwikkelingen (zoals de analyses in de Verenigde Staten naar het gebruik van gestandaardiseerde privacyverklaringen), maar het onderzoek heeft betrekking op privacyverklaringen die op websites worden geplaatst van online winkels die in Nederland zijn gevestigd. Daarbij wordt als vertrekpunt genomen dat de persoonsgegevens in Nederland worden verwerkt. Vanuit dit licht bezien zullen de onderzoeksvragen worden beantwoord naar Nederlands recht.

Het onderzoek is afgesloten op 22 februari 2012.

[26] Groep Gegevensbescherming Artikel 29-2010 (II), p. 3.

Hoofdstuk 2 | De informatieplicht en de privacyverklaring

2.1 Inleiding

In dit hoofdstuk zal aan de hand van literatuur een verkenning worden uitgevoerd naar de in de Wbp opgenomen informatieplicht en zal worden getracht de privacyverklaring als instrument te kwalificeren. Het doel is ten eerste inzicht te krijgen in de mogelijke relatie tussen de informatieplicht en de privacyverklaring. Ten tweede biedt de verkenning aanknopingspunten voor het analysekader ten behoeve van het empirisch onderzoek naar het gebruik van privacyverklaringen op het Internet.[27] De opbouw van dit hoofdstuk is als volgt. In paragraaf 2.2 wordt de informatieplicht uit de Wbp besproken, en wordt tevens ingegaan op de consequenties voor het gebruik van bepaalde technologische applicaties (cookies). Vervolgens komt in paragraaf 2.3 de privacyverklaring aan de orde, waarbij de nadruk ligt op de kenbaarheid, de verschijningsvorm en de inhoud van de privacyverklaring. Paragraaf 2.4 onderzoekt de verantwoordelijkheid van het Cbp ten aanzien van het toezicht op de naleving en handhaving van de informatieplicht. Paragraaf 2.5 bespreekt de rechtsmiddelen die de betrokkene heeft indien de verantwoordelijke zijn informatieplicht jegens hem niet nakomt. Tot slot wordt dit hoofdstuk in paragraaf 2.6 afgesloten met een samenvatting en conclusies.

2.2 De informatieplicht van de verantwoordelijke

2.2.1 Artikelen 33 en 34 Wbp

In de artikelen 33 en 34 Wbp is de informatieplicht geregeld die de verantwoordelijke in acht dient te nemen jegens de betrokkene indien er sprake is van verwerking van persoonsgegevens. Deze artikelen vormen een uitwerking van het transparantiebeginsel en het in artikel 6 Wbp neergelegde 'fair processing' beginsel.[28] Aan de hand van de informatieplicht wordt de betrokkene in staat gesteld om de rechtmatigheid van de verwerking van zijn persoonsgegevens na te gaan en desnoods in rechte af te dwingen.[29] De informatieplicht zoals die volgt uit de artikelen 33 en 34 is van dwingend recht, hetgeen betekent dat contractuele afwijkingen van de wettelijke voorschriften niet toelaatbaar zijn

---

27 Het empirisch onderzoek zal in hoofdstuk 4 aan de orde komen.

28 "De verplichting van de verantwoordelijke op eigen initiatief de betrokkene op de hoogte te stellen van het bestaan van de gegevensverwerking is een belangrijk instrument om het gegevensverkeer voor betrokkenen transparant te maken". Kamerstukken II 1997-1998, 25892, nr. 3, p. 149.

29 Hoving, p.129.

tenzij dat in de wet uitdrukkelijk wordt bepaald.[30] Hoewel in de parlementaire stukken en de literatuur de informatieplicht uit de Wbp veelal wordt beperkt tot de artikelen 33 en 34 Wbp, moet worden gewezen op de informatieplicht die volgt uit artikel 35 Wbp en artikel 41 Wbp.[31] Op grond van artikel 35 lid 1 Wbp heeft de betrokkene het recht zich te wenden tot de verantwoordelijke met het verzoek hem mede te delen of persoonsgegevens van hem worden verwerkt.[32] De verantwoordelijke heeft conform ditzelfde lid de plicht om de betrokkene hieromtrent binnen vier weken schriftelijk te informeren. Bovendien is de verantwoordelijke op grond van artikel 41 lid 3 Wbp gehouden de betrokkene op de hoogte te stellen van het feit dat hij zich kan verzetten tegen het voornemen van de verantwoordelijke om persoonsgegevens aan derden te verstrekken of voor rekening van derden te gebruiken met het oog op werving voor commerciële of charitatieve doelen. In dit hoofdstuk zal ik mij voornamelijk beperken tot de informatieplicht zoals die voor de verantwoordelijke volgt uit de artikelen 33 en 34 Wbp.

Het onderscheid tussen de artikelen 33 en 34 Wbp ligt in de wijze waarop de verantwoordelijke de persoonsgegevens verkrijgt. Artikel 33 Wbp is van toepassing indien de persoonsgegevens worden verkregen van de betrokkene zelf, waarbij de betrokkene actief zijn persoonsgegevens ter beschikking stelt en zich ook welbewust is van het feit dat hij die gegevens verstrekt; de verstrekking moet derhalve zijn beoogd.[33] Artikel 34 Wbp is aan de orde indien de persoonsgegevens op 'een andere wijze', dus buiten de betrokkene om, worden verkregen. Van een andere wijze is bijvoorbeeld sprake indien een bedrijf een adressenbestand van een derde koopt ten behoeve van direct marketing acties. Een ander voorbeeld betreft het aanvragen van een *e*-Card voor een familielid.[34] De aanvrager dient in dat geval het e-mailadres van het betreffende familielid te verstrekken aan het bedrijf dat de

---

30 De MvT benadrukt dat de voorschriften van de Wbp te karakteriseren zijn als dwingend recht. Kamerstukken II 1997-1998, 25892, nr. 3, p. 10. In hoofdstuk 3 zal worden onderzocht of de invulling van de informatieplicht kan plaatsvinden op grond van het overeenkomstenrecht.

31 Deze informatieplichten worden in dit onderzoek gezamenlijk aangeduid als de 'passieve' informatieplicht.

32 Zie voor de omvang van de informatieplicht onder meer twee arresten van de Hoge Raad uit 2007. "Verder volgt uit het voorgaande, dat, anders dan Dexia kennelijk wil betogen, de verantwoordelijke bij de voldoening aan de door art. 35 lid 2 Wbp op de verantwoordelijke gelegde verplichting om aan de betrokkene een volledig overzicht van de verwerkte persoonsgegevens te verschaffen niet kan volstaan met de verstrekking van globale informatie, doch alle relevante informatie over de betrokkene moet verschaffen, hetgeen, afhankelijk van de omstandigheden, vaak zal kunnen - en zo nodig op aanwijzing van de rechter zal moeten – gebeuren door het verstrekken van afschriften, kopieën of uittreksels". HR 29 juni 2007 (*Dexia*) in r.o. 34, met noot van AG Verkade, *JOL* 2007, 474, *NJ* 2007, 638 en *RvdW* 2007, 631. Zo ook HR 29 juni 2007 (*HBU*) in r.o. 3.6, met noot van AG Verkade, *JOL* 2007, 478, *JOR* 2007, 208, *NJ* 2007, 639, *RF* 2007, 70 en *RvdW* 2007, 633. Zie ook Dommering 2007. Het inzagerecht kan op grond van artikel 43 Wbp worden beperkt. Recente uitspraken waarin het inzagerecht op grond van artikel 43 e. Wbp wordt beperkt: Rechtbank Utrecht 17 november 2010 (*Medirisk*), LJN BO5222 en Rechtbank Utrecht 17 november 2010 (*Sint Antonius Ziekenhuis*), LJN BO5227.

33 Kamerstukken II 1997-1998, 25892, nr. 3, p. 156.

34 Zie bijvoorbeeld www.hallmark.nl.

e-Card vervaardigt en deze kaart vervolgens via het Internet beschikbaar stelt aan het betreffende familielid. De MvT geeft ter verduidelijking van de verhouding tussen artikel 33 Wbp en artikel 34 Wbp als voorbeeld de gegevensvergaring met behulp van videocamera's. De gegevensvergaring met behulp van videocamera's valt onder artikel 33 Wbp indien het een kenbare observatie betreft. In dat geval is de betrokkene op de hoogte van de aanwezigheid van de camera's en heeft hij de mogelijkheid zich hieraan te onttrekken. Doet hij dat niet dan kan aangenomen worden dat hij zijn persoonsgegevens voor het desbetreffende doel bewust ter beschikking heeft gesteld, aldus de MvT.[35] Betreft het een niet-kenbare observatie, dan is artikel 34 Wbp van toepassing.

Conform artikel 33 Wbp heeft de verantwoordelijke de plicht om de betrokkene te informeren en wel vóór het moment van de verkrijging van de persoonsgegevens. Zo gebiedt artikel 33 lid 2 Wbp de verantwoordelijke om zowel zijn identiteit bekend te maken als de verwerkingsdoeleinden waarvoor de gegevens bestemd zijn. Interessant in dit verband is lid 3 van artikel 33 Wbp, waarin wordt bepaald dat de verantwoordelijke nadere informatie aan de betrokkene dient te verstrekken ter waarborging van een behoorlijke en zorgvuldige verwerking, echter alleen indien en voor zover dat nodig is gelet op (i) de aard van de gegevens en/of (ii) de omstandigheden waaronder de gegevens worden verkregen en/of (iii) het gebruik dat van de gegevens wordt gemaakt. De MvT expliciteert dat de verantwoordelijke in dergelijke gevallen de betrokkene nader moet informeren opdat er sprake is van een gegevensverkrijging die als rechtmatig kan worden aangemerkt, alsook dat de nadere informatie door de verantwoordelijke dient te worden geboden uit overwegingen van maatschappelijke zorgvuldigheid die de verantwoordelijke ten opzichte van de betrokkene in acht moet nemen.[36] De voorwaarde tot het moeten verstrekken van nadere informatie is een aanvulling op de in hoofdstuk 2 Wbp neergelegde voorwaarden voor de rechtmatigheid van gegevensverwerkingen.[37]

> Artikel 33 Wbp
>
> 1. Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij de betrokkene daarvan reeds op de hoogte is.
> 2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mede.
> 3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het

35 Kamerstukken II 1997-1998, 25892, nr. 3, p. 156.
36 Kamerstukken II 1997-1998, 25892, nr. 3, p. 154.
37 Kamerstukken II 1997-1998, 25892, nr. 3, p. 154.

gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Zoals vermeld is artikel 34 Wbp van toepassing indien de persoonsgegevens buiten de betrokkene om worden verkregen. Artikel 34 lid 1 Wbp maakt de momenten duidelijk waarop de betrokkene door de verantwoordelijke geïnformeerd dient te worden, en wel (i) op het moment van vastlegging van de betreffende gegevens over de betrokkene of (ii) uiterlijk op het moment van de eerste verstrekking wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde. In artikel 34 lid 2 en 3 Wbp is bepaald welke informatie door de verantwoordelijke aan de betrokkene dient te worden verstrekt, waarbij kan worden vastgesteld dat de inhoud van beide bepalingen nagenoeg gelijk is aan die van artikel 33 lid 2 en 3 Wbp.

Artikel 34 Wbp

1. Indien persoonsgegevens worden verkregen op een andere wijze dan bedoeld in artikel 33, deelt de verantwoordelijke de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij deze reeds daarvan op de hoogte is:

a. op het moment van vastlegging van hem betreffende gegevens, of

b. wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.[38]

2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking mede.

3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

4. Het eerste lid is niet van toepassing indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast.

5. Het eerste lid is evenmin van toepassing indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid.

De in artikel 34 Wbp neergelegde verplichting is niet van toepassing indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost

[38] "Deze omschrijving moet aldus worden verstaan dat het gaat om gevallen waarin verstrekking van gegevens aan een derde reeds bij de verkrijging is beoogd en de gegevens dus bestemd waren om aan een derde te worden verstrekt". Kamerstukken II 1997-1998, 25892, nr. 3, p. 155.

(artikel 34 lid 4 Wbp) alsook indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven (artikel 35 lid 5 Wbp).

De in de artikelen 33 en 34 Wbp opgenomen plicht vervalt indien de betrokkene reeds op de hoogte is van de informatie die de verantwoordelijke op grond van artikel 33 lid 2 en 3 Wbp of artikel 34 lid 2 en 3 Wbp zou moeten mededelen. De Vries wijst er in dit verband op dat de verantwoordelijke zich pas ontslagen mag achten van zijn informatieplicht als hij weet dat de betrokkene op de hoogte is van de verwerking, waarbij zij tevens stelt dat de verantwoordelijke niet in alle gevallen dat hij gegevens bij de betrokkene zelf vergaart zich van de bewustzijnsinhoud van de betrokkene hoeft te vergewissen.[39] De MvT verduidelijkt dat de verantwoordelijke op uiteenlopende wijze, afhankelijk van de omstandigheden, mag aannemen dat de betrokkene op de hoogte is van de verwerking. Voorts geeft de MvT aanknopingspunten op grond waarvan de verantwoordelijke mogelijk mag aannemen dat de betrokkene op de hoogte is. Deze luiden als volgt:

(i) het reeds in het bezit zijn van de informatie bij de betrokkene:

> "Beschikt de betrokkene over de informatie, bijvoorbeeld omdat deze hem is overhandigd of toegezonden, dan is hij daarmee op de hoogte, ongeacht of hij het initiatief heeft genomen de informatie ook tot zijn bewustzijn te brengen".[40]

(ii) gedragingen of verklaringen van de betrokkene:

> "Hoewel de verantwoordelijke dus niet zonder meer ervan mag uitgaan dat de betrokkene in een bepaalde situatie wel kan weten of weet dat, door wie en hoe de gegevens worden verwerkt, kunnen ook bepaalde gedragingen of verklaringen van de verantwoordelijke [de MvT bedoelt hier waarschijnlijk de betrokkene] aanleiding geven tot het gerechtvaardigde vermoeden dat de betrokkene daarvan op de hoogte is. Het gaat om gedragingen of verklaringen die in het maatschappelijk verkeer de betrokkene kunnen worden toegerekend als blijk van het feit dat hij op de hoogte is".[41]

> "Als de betrokkene middels een gedraging laat blijken op de hoogte te zijn van de informatie en deze gedraging in het maatschappelijk verkeer ook als zodanig mag worden opgevat, kan van de verantwoordelijke geen verdergaande actie ten aanzien van zijn informatieplicht worden gevergd. De betrokkene kan dan worden toegerekend dat zijn gedraging op die wijze door de verantwoordelijke wordt geïnterpreteerd. Mocht

39 De Vries 2009, art. 33 Wbp, aant. 2., p. 605.
40 Kamerstukken II 1997-1998, 25892, nr. 3, p. 150.
41 Kamerstukken II 1997-1998, 25892, nr. 3, p. 151.

> hij een andere bedoeling hebben gehad met zijn gedragingen dan heeft hij een hem verwijtbaar risico geschapen van een misverstand met de verantwoordelijke".[42]

(iii) de wijze van totstandkoming van het contact tussen de verantwoordelijke en de betrokkene:

> "De omvang van de informatieverplichting is mede afhankelijk van de wijze waarop het contact tot stand komt. In beginsel zal op de verantwoordelijke een extra verantwoordelijkheid tot informeren rusten als hij zelf het initiatief neemt tot het contact met de betrokkene. De betrokkene die de verantwoordelijke zelf benadert, zal veelal reeds op de hoogte zijn van diens identiteit en oogmerken. Dan moet wel nog het concrete doel van de gegevensverwerking en eventueel aanvullende informatie worden verstrekt, terwijl in geval dat redelijkerwijs twijfel mogelijk is, ook de identiteit van de verantwoordelijke dient te worden bekendgemaakt. In de gevallen dat de verantwoordelijke er niet op mag vertrouwen dat de betrokkene op de hoogte is, dient hij ten minste zijn identiteit bekend te maken en de betrokkene te informeren over het doel van de gegevensverwerking".[43]

De betrokkene zelf heeft geen onderzoeksplicht. De gedachte die hieraan ten grondslag ligt is de ongelijkwaardigheid van partijen. Met andere woorden: de wetgever verlegt de balans in het voordeel van de betrokkene, zijnde de in het algemeen maatschappelijk zwakkere partij.[44]

De Wbp kent diverse open normen die nader ingevuld dienen te worden. De artikelen 33 en 34 Wbp bevatten duidelijk een dergelijke open norm, nu niet wordt gepreciseerd wat dient te worden verstaan onder begrippen als: nadere informatie, een behoorlijke en zorgvuldige verwerking en onder aard en/of omstandigheden op grond waarvan die nadere informatie verstrekt zou moeten worden aan de betrokkene. Slechts waar het de identiteit en de doeleinden van de verwerking betreft dient de verantwoordelijke specifiek te zijn. Voor het overige is het aan de verantwoordelijke zelf om te bepalen welke (aanvullende) informatie hij verstrekt aan de betrokkene. De Vries meent dat de verantwoordelijke zich telkens zal moeten afvragen of de omstandigheden met zich meebrengen dat verwacht mag worden dat de betrokkene een reëel belang heeft bij nadere informatie en zo ja, wat de omvang van deze informatie is.[45] Het resultaat van deze afweging kan er echter ook toe leiden dat de verantwoordelijke er voor kiest geen aanvullende informatie aan de betrokkene te

---

42 Kamerstukken II 1997-1998, 25892, nr. 3, p. 151.

43 Kamerstukken II 1997-1998, 25892, nr. 3, p. 151.

44 Kamerstukken II 1997-1998, 25892, nr. 3, p. 150.

45 De Vries 2009, art. 33 Wbp, aant. 4., p. 606. Zo ook Kamerstukken II 1997-1998, 25892, nr. 3, p. 154.

verstrekken omdat hij van oordeel is dat dit 'gelet op de aard van de gegevens', 'de omstandigheden waaronder zij worden verkregen' of 'het gebruik dat ervan wordt gemaakt' niet noodzakelijk is. De verantwoordelijke dient derhalve telkenmale de reikwijdte van zijn informatieplicht te overwegen. De MvT stelt in dit verband dat voor een nader begrip van de reikwijdte van de informatieplicht aansluiting kan worden gezocht bij bestaande noties die in het Nederlands privaatrecht tot ontwikkeling zijn gekomen. Zo wijst de MvT op artikel 6:228 lid 2 BW waarin is bepaald dat iemand zich bij het sluiten van een overeenkomst niet kan beroepen op dwaling, indien deze zijn oorsprong vindt in omstandigheden die volgens de in het verkeer geldende opvattingen voor rekening van de dwalende behoren te komen. Uit de MvT is kortom af te leiden dat de betreffende bepaling uitdrukking geeft aan het beginsel dat bij de totstandkoming van een overeenkomst in het algemeen een balans bestaat tussen de informatieplicht van de één en de onderzoeksplicht van de ander. "Naar welke kant de balans in een concreet geval doorslaat, is afhankelijk van de omstandigheden zoals de deskundigheid van betrokkenen en de wetenschap die men bij elkaar mag veronderstellen. Een dergelijke balans doet zich ook voor in situaties waarin geen sprake is van een overeenkomst", aldus de MvT.[46]

De artikelen 33 en 34 Wbp zijn in de Wbp opgenomen ter implementatie van de artikelen 10 en 11 van de Privacyrichtlijn. In zowel artikel 33 lid 3 Wbp als artikel 34 lid 3 Wbp is wat betreft de te verstrekken informatie gekozen voor de formulering 'nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen'. In de artikelen 10 sub c Richtlijn en 11 lid 1 sub c van de Privacyrichtlijn is daarentegen gekozen voor de bewoording van het moeten doen verstrekken van "verdere informatie zoals de betrokken gegevenscategorieën, de ontvangers of de categorieën ontvangers, het bestaan van een recht op toegang tot zijn eigen persoonsgegevens en op rectificatie van deze gegevens, voor zover die, met inachtneming van de specifieke omstandigheden waaronder de verdere informatie verzameld wordt, nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen". De Nederlandse wetgever heeft er klaarblijkelijk voor gekozen de in de Privacyrichtlijn genoemde voorbeelden wat onder de noemer 'verdere informatie' valt te scharen, niet over te nemen. Ze heeft in plaats daarvan gekozen voor een meer open formulering. In de MvT wordt niet toegelicht wat de Nederlandse wetgever hiertoe heeft doen bewegen. Daarbij dient te worden aangetekend dat Europese lidstaten een zekere bandbreedte hebben bij de inrichting van hun implementatiewetgeving.[47] Dit zou volgens de

---

46 Kamerstukken II 1997-1998, 25892, nr. 3, p. 150.

47 Zie ook HvJEG 6 november 2003 (*Lindqvist*), C-101/01, overweging 97: "Richtlijn 95/46 kent de lidstaten op bepaalde gebieden inderdaad een manoeuvreerruimte toe, en machtigt hen bijzondere regelingen voor specifieke situaties te handhaven of in te voeren, zoals uit een groot aantal van haar bepalingen blijkt. Die mogelijkheden dienen echter op de in richtlijn 95/46 voorgeschreven wijze te worden benut overeenkomstig haar doel dat erin bestaat een evenwicht tussen het vrije

MvT tot gevolg kunnen hebben dat de Privacyrichtlijn niet tot een volledige harmonisatie van de privacywetgeving zal leiden vanwege het feit dat er een zeker minimum en een maximum is dat niet mag worden overschreden.[48] Dat de MvT terecht deze conclusie trok, bleek uit het verslag van de Europese Commissie over de toepassing van de Privacyrichtlijn.[49] In dit verslag is ten aanzien van de toepassing van de artikelen 10 en 11 van de Privacyrichtlijn geconcludeerd dat er zich verschillen voordoen tussen de Europese lidstaten. Naar de visie van de Europese Commissie is dit in zekere mate toe te schrijven aan een incorrecte tenuitvoerlegging, bijvoorbeeld wanneer een wet bepaalt dat altijd aanvullende informatie aan de betrokkene moet worden verstrekt, ongeacht de noodzakelijkheidstest waarin de Privacyrichtlijn voorziet. Voorts zou het ook te maken hebben met uiteenlopende interpretaties en praktijken bij de toezichthoudende autoriteiten.[50] Al met al reden voor de Europese Commissie om een actiepunt te definiëren, met als doel om te komen tot meer geharmoniseerde bepalingen inzake de informatieverstrekking. Dit actiepunt voorzag in een verzoek aan de Groep Gegevensbescherming Artikel 29 om medewerking te verlenen bij het zoeken naar een uniformere interpretatie van artikel 10 van de Privacyrichtlijn[51], hetgeen heeft geresulteerd in een advies dat in paragraaf 2.3.2 aan de orde zal komen.[52]

2.2.2 ePrivacyrichtlijn

Omdat er specifieke en met name zwaardere informatieplichten (die erop neerkomen dat toestemming van de betrokkene noodzakelijk is) gelden voor het gebruik van cookies wordt hier specifiek stilgestaan bij de betreffende bepalingen hieromtrent. Persoonsgegevens kunnen worden verzameld door gebruik te maken van zogeheten 'cookies'. Een cookie is software waarmee, al dan niet heimelijk, persoonsgegevens van de betrokkene kunnen worden verkregen. Cookies kunnen op diverse wijzen worden gecategoriseerd. Zo zijn er allereerst tijdelijke cookies (sessie cookies) en persistente cookies. Tijdelijke cookies worden verwijderd wanneer de webbrowser wordt afgesloten, terwijl persistente cookies juist geïnstalleerd blijven op de computer van de betrokkene. Cookies kunnen hiernaast ook worden onderscheiden in cookies van derden (indirecte cookies of third party cookies) en cookies die door de verantwoordelijke zelf worden geplaatst (first party cookies). Verder bestaan er zogeheten tracking cookies. Aan de hand van tracking cookies kan het surfgedrag van de betrokkene worden gevolgd. Op basis van de, via tracking cookies, verkregen informatie kunnen vervolgens profielen worden opgebouwd. Hierdoor worden

---

verkeer van de persoonsgegevens en de bescherming van de persoonlijke levenssfeer te verzekeren", *NJ* 2004, 248. Zie tevens Dommering die in zijn annotatie bij het *Dexia*-arrest en *HBU*-arrest uitgebreid ingaat op de manoeuvreerruimte ('margin of manoeuvre') die de Privacyrichtlijn aan de lidstaten biedt. Dommering 2007.

48 Kamerstukken II 1997-1998, 25892, nr. 3, p. 5.

49 COM (200) 265 definitief.

50 COM (200) 265 definitief, p. 20.

51 COM (200) 265 definitief, p. 27 e.v.

52 Groep Gegevensbescherming Artikel 29-2004.

bijvoorbeeld adverteerders in staat gesteld om meer doelgerichte reclamecampagnes uit te voeren. Maar ook verzekeringsmaatschappijen kunnen hiermee bijvoorbeeld inzicht verkrijgen in mogelijk risicovolle interesses van de betrokkene.[53] In het actuele debat over het gebruik van cookies wordt met name ingezet op het toestemmingsvereiste, in het bijzonder of de betrokkene zijn toestemming dan wel ondubbelzinnige toestemming dient te verstrekken alvorens een cookie door de verantwoordelijke mag worden geplaatst en uitgelezen. Zoals in het navolgende zal blijken kan toestemming slechts rechtsgeldig worden verstrekt indien de betrokkene vooraf beschikt over alle relevante informatie aangaande het gebruik van cookies. De relatie tussen de informatieplicht, toestemming en cookies zal hierna aan de orde komen.

2.2.2.1 Informatieverstrekking en toestemmingsvereiste

Holleman[54] alsook Tempelman[55] betoogden in 2003 dat bij het gebruik van cookies artikel 34 Wbp van toepassing zou zijn aangezien de persoonsgegevens van de betrokkene via de website indirect worden verkregen. Indien het in de MvT aangehaalde voorbeeld van, al dan niet kenbare, videocameraopnamen wordt geprojecteerd op het gebruik van cookies, dan is het antwoord op de vraag of artikel 33 Wbp dan wel artikel 34 Wbp van toepassing is, afhankelijk van de omstandigheid of de betrokkene al dan niet weet dat er een cookie op zijn computer is geïnstalleerd en of hij zich ervan bewust is dat hij daardoor persoonsgegevens verstrekt.

Op 12 juli 2002 is de Europese richtlijn betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie in werking getreden.[56] Deze richtlijn wordt in de literatuur veelal aangehaald als de *e*Privacyrichtlijn. Op grond van artikel 5 lid 3 *e*Privacyrichtlijn dienen de lidstaten er voor zorg te dragen dat het gebruik van elektronische communicatienetwerken voor de opslag van informatie of voor het verkrijgen van toegang tot informatie die is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken gebruiker wordt voorzien van duidelijke en volledige informatie over de doeleinden van de verwerking overeenkomstig Richtlijn 95/46/EG. Tevens verkrijgt de betrokkene op grond van artikel 5 lid 3 *e*Privacyrichtlijn het recht om een dergelijke verwerking te weigeren.

---

53 Zie in dit kader Prins die wijst op de 'digital footprint' van burgers (gegevens die zij al dan niet bewust c.q. vrijwillig zelf genereren), en de 'digital shadow' van burgers (informatie die anderen uit hun gedrag afleiden). Prins 2011, p. 107.

54 Holleman 2003, p. 254.

55 Tempelman, p. 199.

56 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), PbEG L 201/37.

Artikel 5 lid 3 *e*Privacyrichtlijn

De lidstaten dragen er zorg voor dat het gebruik van elektronische communicatienetwerken voor de opslag van informatie of voor het verkrijgen van toegang tot informatie die is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken gebruiker voorzien wordt van duidelijke en volledige informatie onder andere over de doeleinden van de verwerking, overeenkomstig Richtlijn 95/46/EG, en het recht krijgt aangeboden door de voor de verwerking verantwoordelijke om een dergelijke verwerking te weigeren. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering of vergemakkelijking van de verzending van een communicatie over een elektronische-communicatienetwerk, of, indien strikt noodzakelijk, voor de levering van een uitdrukkelijk door de abonneegebruiker gevraagde dienst van de informatiemaatschappij.

Op 7 mei 2004 is het Besluit universele dienstverlening en eindgebruikersbelangen (Bude) in werking getreden.[57] Ter implementatie van artikel 5 lid 3 van de *e*Privacyrichtlijn is in artikel 4.1 lid 1 Bude een regeling opgenomen die voorwaarden stelt aan het verkrijgen van toegang tot gegevens die in de apparatuur van gebruikers staan. In dit artikel is bepaald dat een ieder die door middel van elektronische communicatienetwerken gegevens wenst op te slaan in de randapparatuur van de abonnee of gebruiker van openbare elektronische communicatiediensten, *voorafgaand* aan de desbetreffende handeling de abonnee of gebruiker op een duidelijke en nauwkeurige wijze dient te informeren omtrent de doeleinden waarvoor men gegevens wenst op te slaan en hem op een voldoende kenbare wijze gelegenheid te bieden de desbetreffende handeling te weigeren.

Artikel 4.1 lid 1 Bude

Een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een abonnee of gebruiker van openbare elektronische communicatiediensten dan wel gegevens wenst op te slaan in de randapparatuur van de abonnee of gebruiker van openbare elektronische communicatiediensten, dient voorafgaand aan de desbetreffende handeling de abonnee of gebruiker:

a. op een duidelijke en nauwkeurige wijze te informeren omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en

b. op voldoende kenbare wijze gelegenheid te bieden de desbetreffende handeling te weigeren.

---

57 Besluit van 7 mei 2004, Stb. 203, houdende regels met betrekking tot universele dienstverlening en eindgebruikersbelangen.

Artikel 4.1 Bude lijkt af te wijken van de *e*Privacyrichtlijn, aangezien dit artikel voorschrijft dat de betrokkene geïnformeerd dient te worden *voordat* de cookie wordt geplaatst, terwijl in de *e*Privacyrichtlijn het moment van informeren niet nader wordt geregeld. In de praktijk heeft de werking van artikel 4.1 Bude tot gevolg dat de betrokkene door de verantwoordelijke geïnformeerd dient te worden voordat hij toegang verkrijgt tot de website van de verantwoordelijke; een cookie wordt veelal geplaatst direct bij het openen van de website. Tevens dient de betrokkene in dat geval de mogelijkheid te hebben om aan te geven of hij wel of niet instemt met het gebruik van cookies.

Artikel 5 lid 3 *e*Privacyrichtlijn maakt niet duidelijk of de betrokkene vooraf geïnformeerd dient te worden en/of dat hij zijn toestemming moet hebben gegeven alvorens de cookie mag worden geplaatst. Op 25 november 2009 is artikel 5 lid 3 van de *e*Privacyrichtlijn gewijzigd. Op grond van dit gewijzigde artikel blijkt dat het plaatsen van een cookie slechts is toegestaan indien de betrokkene zijn toestemming heeft verleend nadat hij is voorzien van duidelijke en volledige informatie.[58]

> Gewijzigd Artikel 5 lid 3 *e*Privacyrichtlijn
> De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig Richtlijn 95/46/EG, onder meer over de doeleinden van de verwerking. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert.

Het gewijzigde artikel 5 lid 3 *e*Privacyrichtlijn maakt niet duidelijk op welk moment de betrokkene zijn toestemming dient te verstrekken. Naar de mening van de Groep Gegevensbescherming Artikel 29 verduidelijken en versterken de veranderingen in het nieuwe artikel 5 lid 3 *e*Privacyrichtlijn de noodzaak van voorafgaande toestemming. Dit wordt volgens de Groep op twee manieren gedaan. Ten eerste door de formulering ‘het recht (…) te weigeren’ te vervangen door de noodzaak ‘toestemming’ te verkrijgen, zoals

---

58 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, PbEG L337/11.

beschreven in Richtlijn 95/46/EG, en door het gebruik van de voltooid tegenwoordige tijd 'te zijn voorzien'.[59] In de opinie uit 2011 herhaalt de Groep Gegevensbescherming Artikel 29 dat voorafgaande toestemming een vereiste is. "While Article 5(3) does not use the word prior, this is a clear and obvious conclusion from the wording of the provision".[60]

Er is een brede maatschappelijke discussie gaande over de vraag wat er exact moet worden verstaan onder 'toestemming'. Dit heeft alles te maken met het feit dat in het gewijzigde artikel 5 lid 3 *e*Privacyrichtlijn wordt verwezen naar de Privacyrichtlijn. De Privacyrichtlijn onderscheidt drie varianten van toestemming, te weten 'toestemming', 'ondubbelzinnige toestemming' en 'uitdrukkelijke toestemming'.[61] Ook de Wbp onderscheidt deze toestemmingsvarianten. Alvorens het verloop van de discussie omtrent het toestemmingsvereiste te duiden, zal worden ingegaan op de varianten 'toestemming' en 'ondubbelzinnige toestemming' zoals die in de Wbp zijn opgenomen.

In artikel 1 sub i. Wbp wordt 'toestemming' van de betrokkene gedefinieerd als elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt. De MvT expliciteert dat er drie punten essentieel zijn om te kunnen spreken van toestemming van de betrokkene:[62]

1. De betrokkene moet in vrijheid zijn wil kunnen uiten;
2. De wilsuiting moet betrekking hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen; en
3. De betrokkene moet voor een goede oordeelsvorming over de noodzakelijke inlichtingen beschikken.

In de navolgende tabellen worden deze drie punten verduidelijkt.

Voorwaarde 1: In vrijheid uiten van de wil[63]
• "De betrokkene moet in vrijheid zijn wil met betrekking tot de betreffende gegevensverwerking kunnen uiten, en deze wil dient ook daadwerkelijk geuit te zijn. • De artikelen 3:33 en 3:35 BW zijn in dezen van overeenkomstige toepassing, aangezien artikel 3:59 BW immers bepaalt dat deze bepalingen op een overeenkomstige wijze worden toegepast voor zover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet.

59 Groep Gegevensbescherming Artikel 29-2010, p. 14. Zie in dit kader ook het Working Document van het Communications Committee van de Europese Commissie: European Commission, Communications Committee, Working Document 'Implementation of the revised Framework-Article 5(3) of the ePrivacy Directive, COCOM10-34, Brussels, 20 October 2010.

60 Groep Gegevensbescherming Artikel 29-2011, p. 31.

61 Zie in dit kader ook Schreuders die uitgebreid ingaat op de diverse toestemmingsvarianten zoals die zijn opgenomen in de Privacyrichtlijn en ePrivacyrichtlijn. Zie tevens de opinie van de Groep Gegevensbescherming Artikel 29-2011.

62 Kamerstukken II 1997-1998, 25892, nr. 3, p. 65.

63 Kamerstukken II 1997-1998, 25892, nr. 3, p. 65.

- Er kan bijvoorbeeld niet van een rechtsgeldige toestemming worden gesproken als de betrokkene onder druk van omstandigheden waarin hij verkeert of de relatie waarin hij staat tot de verantwoordelijke, tot toestemming is overgegaan".

Tabel 2.1

Voorwaarde 2: De wilsuiting moet betrekking hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen[64]

- "Duidelijk moet zijn welke verwerking, van welke gegevens, voor welk doel zal plaatsvinden, en als het daarbij gaat om een verstrekking aan derden, ook aan welke derden.
- Een zeer brede en onbepaalde machtiging tot het verwerken van gegevens kan niet als zodanig worden aangemerkt.
- De betrokkene moet weten om welke gegevensverwerking het gaat en hiervoor gerichte toestemming geven.
- Er kan evenmin van een rechtsgeldige toestemming worden gesproken wanneer de betrokkene geconfronteerd wordt met een geheel andere gegevensverwerking dan waarvoor hij toestemming had verleend".

Tabel 2.2

Voorwaarde 3: Beschikken over noodzakelijke gegevens[65]

- "De betrokkene kan slechts verantwoord zijn toestemming geven wanneer hij zo goed mogelijk is ingelicht.
- Het vragen van de toestemming van de betrokkene impliceert dat hij op de hoogte moet worden gesteld van de gang van zaken met betrekking tot de gegevensverwerking.
- De betrokkene moet voldoende en begrijpelijk door de verantwoordelijke worden geïnformeerd over de verschillende aspecten van de gegevensverwerking die voor hem van belang zijn.
- De informatieplicht van de verantwoordelijke wordt begrensd door de feiten die de betrokkene reeds kent of zou moeten kennen.
- De informatieplicht van de verantwoordelijke impliceert niet dat de betrokkene geen enkele verantwoordelijkheid draagt. De betrokkene heeft een zekere onderzoeksplicht voor hij een oordeel geeft.
- Bepalend voor de mate waarin de verantwoordelijke de betrokkene moet informeren, dan wel de betrokkene zelf op onderzoek moet uitgaan, is wat in het maatschappelijk verkeer redelijkerwijs over en weer van elkaar mag worden verwacht.
- Factoren die bij weging een rol kunnen spelen zijn de soort gegevens, de verwerkingen die de verantwoordelijke wil verrichten alsmede de context waarin deze verwerkingen

64 Kamerstukken II 1997-1998, 25892, nr. 3, p. 65.

65 Kamerstukken II 1997-1998, 25892, nr. 3, p. 65 e.v.

zullen plaatsvinden, de eventuele derden aan wie de gegevens kunnen worden verstrekt enz., maar ook de maatschappelijke positie en onderlinge verhouding tussen de verantwoordelijke en de betrokkene alsmede de wijze waarop zij met elkaar in contact zijn getreden".

Tabel 2.3

De aanvullende vereisten op het begrip 'toestemming' opdat er sprake is van een 'ondubbelzinnige toestemming', luiden conform het bepaalde in de MvT als volgt:[66]

Voorwaarde 4: Aanvullende vereisten op het begrip toestemming opdat er sprake is van 'ondubbelzinnige toestemming'
• "De verantwoordelijke mag niet uitgaan van toestemming indien hij geen opmerkingen maakt over de gegevensverwerking, daarbij uitgaande van de kennis die hij op grond van maatschappelijke opvattingen redelijkerwijs bij de betrokkene aanwezig mag achten. • Elke twijfel moet bij de verantwoordelijke zijn uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven en voor welke specifieke verwerkingen deze toestemming is gegeven. • Op de verantwoordelijke zal doorgaans een verdergaande informatieverplichting rusten. • Bij twijfel over de vraag of de betrokkene zijn toestemming heeft verleend dient de verantwoordelijke te verifiëren of hij er terecht vanuit gaat dat de betrokkene er mee heeft ingestemd. • Bij interactieve diensten zal bijvoorbeeld de klik met de muis of een aanslag op het toetsenbord van de computer ten einde de (koop-) overeenkomst te sluiten (veelal nog gevolgd door een aparte klik voor de bevestiging van de koopovereenkomst), als ondubbelzinnige toestemming kunnen worden aangemerkt".

Tabel 2.4

Uit het wetsvoorstel voor wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen blijkt dat op grond van het beoogde artikel 11.7a lid 1 Telecommunicatiewet de verantwoordelijke, indien hij een cookie wil plaatsen op de computer van de betrokkene, (i) de betrokkene duidelijk en volledig dient te informeren conform de Wbp, en in ieder geval over de doeleinden waarom hij die cookie wil plaatsen, en (ii) toestemming van de betrokkene dient te hebben verkregen om de cookie te mogen plaatsen.[67]

66 Kamerstukken II 1997-1998, 25892, nr. 3, p. 66 e.v.

67 Kamerstukken II 2010-2011, 32549, nr. 2, p. 21.

Wetsvoorstel Artikel 11.7a Telecommunicatiewet

1. Een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een gebruiker dan wel gegevens wenst op te slaan in de randapparatuur van de gebruiker, dient:

a. de gebruiker duidelijke en volledige informatie te verstrekken overeenkomstig de Wet bescherming persoonsgegevens, en in ieder geval omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en

b. van de gebruiker toestemming te hebben verkregen voor de desbetreffende handeling.

2. De in het eerste lid, onder a en b, genoemde vereisten zijn ook van toepassing in het geval op een andere wijze dan door middel van een elektronisch communicatienetwerk wordt bewerkstelligd dat via een elektronisch communicatienetwerk gegevens worden opgeslagen of toegang wordt verleend tot op het randapparaat opgeslagen gegevens.

3. Het bepaalde in het eerste en tweede lid is niet van toepassing, voor zover het de technische opslag of toegang tot gegevens betreft met als uitsluitend doel:

a. de communicatie over een elektronisch communicatienetwerk uit te voeren, of

b. de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is.

4. Bij algemene maatregel van bestuur kunnen in overeenstemming met Onze Minister van Justitie nadere regels worden gegeven met betrekking tot de in het eerste lid, onder a en b, genoemde vereisten. Het College bescherming persoonsgegevens wordt om advies gevraagd over een ontwerp van bedoelde algemene maatregel van bestuur.

In de MvT behorend bij het wetsvoorstel voor wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen wordt geëxpliciteerd dat de verantwoordelijke geen 'ondubbelzinnige toestemming' van de betrokkene hoeft te hebben om de cookie te mogen plaatsen.[68] Het kabinet is van mening dat een vereiste van 'ondubbelzinnige toestemming' verder gaat dan de *e*Privacyrichtlijn voorschrijft, en dat dientengevolge de concepttekst van artikel 11.7a Telecommunicatiewet is aangepast.[69] In dezen heeft het kabinet zich tevens laten leiden door de kritiek dat een vereiste van 'ondubbelzinnige toestemming' tot gevolg zou hebben dat (i) het Internet gebruiksonvriendelijk zou worden, dat (ii) in de praktijk de gebruiker steeds toestemming zal verlenen zonder zich te realiseren waarvoor, dat (iii) er juist meer persoonsgegevens geregistreerd moeten worden door degene die verantwoordelijk is voor de cookies, en (iv) dat het zou leiden tot economische schade voor de hele internetsector.[70] De MvT laat zich

68 Kamerstukken II 2010-2011, 32549, nr. 3, p. 41.

69 Kamerstukken II 2010-2011, 32549, nr. 3, p. 41. Zo ook Kamerstukken II 2010-2011, 32549, nr. 7, p. 25.

70 Kamerstukken II 2010-2011, 32549, nr. 3, p. 41.

niet uit over de wijze waarop de betrokkene zijn toestemming dient te geven. Anderzijds wordt in de MvT gerefereerd aan de, volgens de MvT, breed gedragen oplossing om de browserinstelling van de gebruiker bepalend te laten zijn voor de vraag of de gebruiker de vereiste toestemming voor het plaatsen en lezen van cookies heeft gegeven.[71] Het kabinet lijkt echter niet voor een dergelijke oplossing te willen kiezen.[72]

De vaste commissie van de Tweede Kamer heeft schriftelijke vragen gesteld naar aanleiding van het wetsvoorstel van het kabinet.[73] De vragen zien in het bijzonder op de benodigde toestemmingsvariant, de wijze waarop toestemming kan worden verstrekt en de wijze van informatieverstrekking aan de betrokkene over het gebruik van cookies. Zo vragen bijvoorbeeld de leden van de PvdA-fractie zich af of de maatregelen ter bescherming van de persoonsgegevens, zoals voorgesteld in artikel 11.7a eerste lid, wel ver genoeg gaan. Voorts wil deze fractie weten waarom de regering niet heeft gekozen voor de termen 'geïnformeerde toestemming' en 'uitdrukkelijke toestemming'. Tevens informeren ze of het niet juist van belang is dat consumenten weten welke persoonsgegevens van hen verzameld worden en zij daarvoor uitdrukkelijk toestemming dienen te verlenen. Tenslotte vraagt deze fractie zich af of de door de regering gekozen formulering niet teveel ruimte laat om middels een algemene toestemming voor het plaatsen van cookies allerhande persoonsgegevens op te slaan en door te geven.[74] De leden van de D66-fractie stellen dat in artikel 5 lid 3 van de *e*Privacyrichtlijn de nadruk wordt gelegd op het leveren van voorafgaande informatie en het verkrijgen van voorafgaande toestemming (voorafgaand aan het begin van de verwerking). Zij vragen de regering om "duidelijker te zijn over de manier waarop de informatie moet worden verstrekt, nu in de MvT van het onderhavige wetsvoorstel hier met geen woord over wordt gerept". Tevens stelt deze fractie dat artikel 11.7a. van het wetsvoorstel zelf niet duidelijk is, en vragen de leden zich af of de regering zich ervan bewust is dat alleen voorafgaande informatieverstrekking in lijn is met de richtlijnen betreffende e-privacy en gegevensbescherming.[75]
In reactie op de vragen van de vaste commissie herhaalt en beargumenteert het kabinet het standpunt dat 'ondubbelzinnige toestemming' voor het plaatsen en lezen van een cookie geen vereiste is, alsook waarom dit standpunt in lijn zou zijn met de Privacyrichtlijn en de *e*Privacyrichtlijn.[76] Met betrekking tot de informatieverstrekking aan de betrokkene onderkent het kabinet dat deze tevens in lijn dient te zijn met de Privacyrichtlijn. Over de

71 Kamerstukken II 2010-2011, 32549, nr. 3, p. 41.
72 Zie ook Groep Gegevensbescherming Artikel 29-2010, p. 15, waarin voorwaarden met betrekking tot de browserinstellingen worden geformuleerd op basis waarvan de verantwoordelijke mag aannemen dat de betrokkene zijn toestemming heeft gegeven.
73 Kamerstukken II 2010-2011, 32549, nr. 6.
74 Kamerstukken II 2010-2011, 32549, nr. 6, p. 10 e.v.
75 Kamerstukken II 2010-2011, 32549, nr. 6, p. 11.
76 Kamerstukken II 2010-2011, 32549, nr. 7, p. 25.

wijze waarop de verantwoordelijke de benodigde informatie moet verstrekken, laat het kabinet zich in beperkte mate uit.

In het debat over het toestemmingsvereiste heeft het Cbp afstand genomen van de visie van het kabinet dat 'ondubbelzinnige toestemming' niet vereist zou zijn. Het College stelt dat voor het plaatsen van cookies 'ondubbelzinnige toestemming' noodzakelijk is: "De enige conclusie die uit beide richtlijnen getrokken kan worden is dat er ondubbelzinnige toestemming is vereist voor het plaatsen en uitlezen van cookies omdat dat in vrijwel alle gevallen leidt tot een verwerking van persoonsgegevens".[77] Ook de OPTA heeft zich in de discussie gemengd, en stelt dat een consument vooraf om toestemming moet worden gevraagd, dat wil zeggen voordat er een cookie wordt geïnstalleerd op zijn computer of andere randapparatuur.[78] Tevens heeft de OPTA laten onderzoeken hoe praktisch invulling kan worden gegeven aan het toestemmingsvereiste. Het onderzoek is uitgevoerd door TNO/IViR. Met betrekking tot het toestemmingsvereiste wordt door TNO/IViR geconcludeerd dat het gewijzigde artikel 5 lid 3 *e*Privacyrichtlijn weinig gevolgen zal hebben voor de Nederlandse wetgeving. "In Nederland verandert er weinig door de implementatie van deze wijziging aangezien de huidige implementatie van de oude regels in artikel 4.1 BUDE reeds een opt-in systeem kent".[79] De opzet en uitkomsten van het TNO/IViR onderzoek gaven aanleiding tot discussie. Met name vanuit de Nederlandse online advertentiemarkt is kritiek geleverd op het rapport.[80]

In het debat tussen het kabinet en de Tweede Kamer over de wijziging van de Telecommunicatiewet is ook nader gediscussieerd over het onderwerp 'toestemming' in relatie tot het plaatsen en uitlezen van cookies. Op grond van het amendement van Van Bemmel/Van Dam[81] wordt artikel 11.7a lid 1 Telecommunicatiewet gewijzigd:[82]

---

77 Cbp Wetgevingsadvies, p. 4 e.v. Zie ook Cbp Brief aan Vaste Commissie, p. 3.

78 OPTA, Persbericht, OPTA's Focus op 2011: "Bezuinigingen dwingen tot keuzes", publicatiedatum 18-01-2011.

79 TNO/IViR, p. 26.

80 De kritiek richt zich op de representativiteit van het rapport en de aannames die gedaan worden op basis van een te kleine populatie. Daarnaast wordt er volgens de branche een onjuiste voorstelling gegeven van de huidige geldende wetgeving. Zo is de branche van mening dat ten onrechte wordt gesteld dat toestemming op grond van de huidige wetgeving (Bude) is vereist. Tevens stelt de branche dat TNO/IViR artikelen verkeerd interpreteert: "De onderzoekers geven op meerdere plaatsen in het rapport ten onrechte aan dat art 5.3 E-Privacy Richtlijn en artikel 4.1 Bude een voorafgaande informatie en/of toestemmingsvereiste kennen (paragraaf 2.1.2, 2.1.3) Dit is onjuist. In beide bepalingen is geen sprake van 'voorafgaand', juist omdat de aard van het internet dit niet toelaat". De branche verzoekt de vaste commissie dan ook om het rapport in de huidige vorm niet mee te nemen in de besluitvorming over de implementatie van de ePrivacyrichtlijn in de Telecommunicatiewet. Branchereactie TNO/IViR Rapport, p. 1 e.v. Naar de mening van De Vries was als gevolg van de conclusie van TNO/IViR de verwarring rond het toestemmingsvereiste compleet. De Vries 2011, p. 184.

81 Kamerstukken II 2010-2011, 32549, nr. 39 (Nader gewijzigd amendement van de leden Van Bemmel en Van Dam ter vervanging van dat gedrukt onder nr. 34) zoals aangenomen op 22 juni 2006, Handelingen Tweede Kamer 2010-2011, nr. 96, item 5, datum vergadering: 22-06-2011. Aan

> Wetsvoorstel Artikel 11.7a lid 1 Telecommunicatiewet o.g.v. Van Bemmel/Van Dam
> 1. Onverminderd de Wet bescherming persoonsgegevens dient een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een gebruiker dan wel gegevens wenst op te slaan in de randapparatuur van de gebruiker:
> a. de gebruiker duidelijke en volledige informatie te verstrekken overeenkomstig de Wet bescherming persoonsgegevens, en in ieder geval omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en
> b. van de gebruiker toestemming te hebben verkregen voor de desbetreffende handeling. Een handeling als bedoeld in de aanhef, die tot doel heeft gegevens over het gebruik van verschillende diensten van de informatiemaatschappij door de gebruiker of de abonnee te verzamelen, combineren of analyseren voor commerciële, charitatieve of ideële doeleinden, wordt vermoed een verwerking van persoonsgegevens te zijn, als bedoeld in artikel 1, onderdeel b, van de Wet bescherming persoonsgegevens.

Hoewel in het eerste lid van artikel 11.7a Telecommunicatiewet is gekozen voor de term 'toestemming', is op grond van de in het betreffende lid opgenomen verwijzing naar de Wbp 'ondubbelzinnige toestemming' vereist indien de cookie wordt gebruikt voor het verzamelen, combineren of analyseren voor commerciële, charitatieve of ideële doeleinden. "Daarmee gaat voor deze categorie handelingen, waarvan het plaatsen en uitlezen van zogeheten tracking cookies de meest bekende is, het strengere regime van de Wbp gelden. Dat wil zeggen dat de gebruiker een 'ondubbelzinnige toestemming' moet verstrekken".[83] Op basis van het amendement van Van Bemmel/Van Dam is er sprake van een omkering van de bewijslast. Immers, elke handeling zoals bedoeld in de aanhef van artikel 11.7a TW wordt vermoed een verwerking van persoonsgegevens te zijn. De minister van Economische Zaken stelt in reactie op het aangenomen amendement dat het "bezwaarlijk blijft dat de bewijslast over de vraag of bij het gebruik van tracking cookies daadwerkelijk persoonsgegevens worden verwerkt altijd bij de gebruiker van tracking cookies ligt, in afwijking van de bestaande privacyregels. Dit gaat ook duidelijk verder dan de richtlijn en zal ertoe leiden dat er verschillende nationale regimes ontstaan".[84]

---

dit amendement gingen twee amendementen vooraf: Kamerstukken II 2010-2011, 32549, nr. 14 en Kamerstukken II 2010-2011, 32549, nr. 34.

82 Kamerstukken I 2010-2011, 32549, nr. A.

83 Kamerstukken II 2010-2011, 32549, nr. 39, p. 2.

84 Kamerstukken II 2010-2011, 32549, nr. 43, p. 2.

Het wetsvoorstel Wijziging van de Telecommunicatiewet is in de Eerste Kamer aan de orde gekomen ter vergadering van 13 september 2011.[85] In het kader van het voorbereidend debat hadden de fracties van de vaste commissies voor Economische Zaken, Landbouw en Innovatie, en voor Infrastructuur, Milieu en Ruimtelijke Ordening diverse vragen ingediend.[86] Deze zien onder meer op de verhouding tussen artikel 11.7a Telecommunicatiewet en het Europese recht, de reikwijdte van de wet en de verhouding tussen artikel 11.7a Telecommunicatiewet en de Wbp.

> VVD-fractie: "Hoe verhoudt de cookiebepaling zich tot het EU recht, nu zij verder gaat dan de e-Privacyrichtlijn, welke volledige harmonisatie beoogt?"[87]
>
> PvdA-fractie: "Kan de regering nader ingaan op de reikwijdte van de wet? Welke soorten cookies vallen onder het toestemmingsvereiste?"[88]
>
> CDA-fractie: "Artikel 5 lid 3 lijkt dus niet bedoeld te zijn voor de uitleg van regels van de Data protectie richtlijn (95/46/EC), of de interpretatie van het begrip persoonsgegeven. Zien de leden van de CDA-fractie dit juist?"
> "Verder vermeldt de uitleg bij het tweede lid van artikel 11.7a, tweede lid, dat zelfs wanneer niet kan worden bewezen dat in de strikte zin van het woord persoonsgegevens worden verzameld of verwerkt, deze handelingen tóch worden aangemerkt als het verzamelen of verwerken van persoonsgegevens in de zin van de Wbp. De leden van de CDA-fractie vragen zich af of dit niet een vergaande oprekking is van het begrip persoonsgegeven en daarmee van de reikwijdte van de Wbp. Wat is het oordeel van de regering hierover?"
> "Door een ondubbelzinnige toestemming voor de verwerking van persoonsgegevens te vereisen doorkruist de wetgever het systeem van de Wbp en stelt een zwaardere eis dan artikel 5(3) van Richtlijn 2009/136/EG. Zien de leden van de fractie van het CDA dit juist?"[89]

---

85 Vergadering van de vaste commissies voor Economische Zaken, Landbouw en Innovatie en Infrastructuur, Milieu en Ruimtelijke Ordening, Korte aantekeningen, 13 september 2011. Het Voorbereidend onderzoek stond geagendeerd op 4 oktober 2011. Het besluit om het wetsvoorstel inhoudelijk te gaan behandelen is ongetwijfeld naar tevredenheid van de lobby van adverteerders. Diverse organisaties zoals de Bond van Adverteerders, Centrum voor Merk en Communicatie, Dutch Dialogue Marketing Association, Nederlands Uitgevers Verbond en Thuiswinkel.org hebben gezamenlijk getracht om de Eerste Kamer te bewegen om het wetsvoorstel inhoudelijk te behandelen, aangezien zij het niet eens waren met het wetsvoorstel. Brief Aan de leden van de Eerste Kamer der Staten Generaal d.d. 3 juli 2011.

86 Kamerstukken I 2011-2012, 32549, nr. B.

87 Kamerstukken I 2011-2012, 32549, nr. B, p. 3.

88 Kamerstukken I 2011-2012, 32549, nr. B, p. 5.

89 Kamerstukken I 2011-2012, 32549, nr. B, p. 6.

In de beantwoording van de vragen door het kabinet wordt bevestigd dat artikel 11.7a Telecommunicatiewet niet verder gaat dan hetgeen de Privacyrichtlijn c.q. de *e*Privacyrichtlijn vereist. Voorts stelt het kabinet dat dit artikel niets afdoet aan de werking van de Wbp, en dat ondubbelzinnige toestemming van de betrokkene is vereist indien aan de hand van cookies persoonsgegevens worden verwerkt.

> "De aangenomen versie van het amendement (32 549, nr. 39) is anders geformuleerd: het amendement verduidelijkt ten eerste dat artikel 11.7a Tw niets afdoet aan de werking van de Wet bescherming persoonsgegevens. Deze toevoeging verwijst naar de reeds bestaande verhouding tussen deze regimes zowel op nationaal als Europees niveau en wijkt dus niet af van de richtlijnen".[90]

> "In overeenstemming met de richtlijnen komt ondubbelzinnige toestemming alleen aan de orde bij verwerking van persoonsgegevens, en is voor cookies waarbij geen sprake is van verwerking van persoonsgegevens «gewone» toestemming vereist".[91]

> "Zoals gezegd is in het voorgestelde artikel 11.7a Tw slechts een omkering van de bewijslast opgenomen voor de vraag of er daadwerkelijk sprake is van verwerking van persoonsgegevens. Anders dan de leden van het CDA stellen is de Wet bescherming persoonsgegevens dus niet van toepassing als er geen persoonsgegevens worden verwerkt. Dat er bij het gebruik van tracking cookies geen persoonsgegevens worden gebruikt moet alleen door degene die die cookies plaatst of leest worden aangetoond, in plaats van andersom (waarbij de betrokkene of het College bescherming persoonsgegevens moeten bewijzen dat er wél persoonsgegevens worden verwerkt)".[92]

Het huidige artikel 4.1 Bude diende uiterlijk op 25 mei 2011 te zijn vervangen door artikel 11.7a in de Telecommunicatiewet.[93] Naar verwachting zal dit artikel in de loop van 2012 in werking treden.[94]

---

90 Kamerstukken I 2011-2012, 32549, nr. E, p. 5. Ook in de Nadere Memorie van Antwoord wordt herhaald dat de uiteindelijke tekst van artikel 11.7a Telecommunicatiewet materieel niet afwijkt van de Europese wetgeving. Kamerstukken I 2011-2012, 32549, nr, G, p. 5. De Nadere Memorie van Antwoord volgt op nader gestelde vragen van de Eerste Kamer commissies. Kamerstukken I 2011-2012, 32549, nr. F.

91 Kamerstukken I 2011-2012, 32549, nr. E, p. 7.

92 Kamerstukken I 2011-2012, 32549, nr. E, p. 8 e.v.

93 Op grond van artikel 4 *e*Privacyrichtlijn dienen de lidstaten uiterlijk op 25 mei 2011 de nodige wettelijke en bestuursrechtelijke bepalingen te implementeren om de richtlijn om te zetten.

94 De Eerste Kamercommissies voor IMRO en voor EL&I hebben op 21 februari 2012 het eindverslag uitgebracht. Kamerstukken I, 2011-2012, 32549, nr. H.

2.2.2.2 Verhouding tussen de informatieplicht uit de Wbp en artikel 11.7a Telecommunicatiewet

Uit de voorgaande paragraaf is gebleken dat de vereiste 'toestemming' zoals opgenomen in artikel 11.7a Telecommunicatiewet dient te worden verstrekt voorafgaand aan het plaatsen van een cookie, en dat de toestemming van de betrokkene ondubbelzinnig dient te zijn (behoudens de uitzondering zoals bedoeld in lid 3 van het desbetreffende artikel). De vraag is vervolgens of de informatieplicht uit de Wbp werking heeft op artikel 11.7a Telecommunicatiewet. Het antwoord is bevestigend. In artikel 11.7a lid 1 onder a. Telecommunicatiewet wordt geëxpliciteerd dat aan de gebruiker duidelijke en volledige informatie dient te worden verstrekt overeenkomstig de Wbp. Ook uit de toelichting bij het amendement van Van Bemmel/Van Dam volgt dat artikel 11.7a Telecommunicatiewet niets afdoet aan de werking van de Wbp.[95] Eerder werd de verhouding tussen de Wbp en artikel 11.7a Telecommunicatiewet door het Cbp verduidelijkt in diens wetgevingsadvies.[96] In dit advies van 4 juni 2010 verduidelijkt het Cbp dat "de toestemming en informatieplicht van artikel 11.7a Telecommunicatiewet mede moet worden uitgelegd en ingevuld met het oog op de algemene toestemmingseis van artikel 8 Wbp en de algemene informatieplicht van artikel 33 Wbp".[97] In de MvT wordt eenzelfde opvatting neergelegd. "Het verstrekken van de informatie bedoeld in het eerste lid betreft in het geval er persoonsgegevens worden verwerkt een specifieke invulling van de informatieplicht die al bestaat op grond van de Algemene privacy-richtlijn, welke is geïmplementeerd in de Wbp", en "Betreft de opgeslagen en later weer gelezen informatie persoonsgegevens in de zin van de Wbp, dan zal de gebruiker, zoals gezegd, voor de verwerking daarvan geïnformeerd moeten worden overeenkomstig de Wbp".[98] Ook de Groep Gegevensbescherming Artikel 29 stelt dat via cookies verzamelde informatie kan worden beschouwd als persoonsgegevens, waarop behalve artikel 5 lid 3 van de *e*Privacyrichtlijn, ook de Richtlijn 95/46/EG van toepassing is.[99] In dit kader wijst de Groep erop dat de beginselen op het gebied van gegevenskwaliteit, de rechten van de betrokkene (zoals toegang, verwijdering, recht op bezwaar), vertrouwelijkheid en veiligheid van de verwerking en internationale overdracht van gegevens onverkort van toepassing zijn.[100] Deze visie is door de Groep Gegevensbescherming Artikel 29 herhaald in een opinie uit 2011. "It should be noted that the Directives are not exclusive of each other. The general conditions for consent to be valid, as foreseen in Directive 95/46/EC, apply both in the off-line and in the on-line world. Directive 2002/58/EC specifies

95 Kamerstukken II 2010-2011, 32549, nr. 39, p. 1. Dat artikel 11.7a Telecommunicatiewet niets afdoet aan de werking van de Wbp volgt tevens uit Kamerstukken I 2011-2012, 32549, nr, E, p. 5.

96 Conform artikel 51 lid 2 Wbp heeft de wetgever het Cbp om advies gevraagd. Kamerstukken II 2010-2011, 32549, nr. 3, p. 43.

97 Cbp Wetgevingsadvies, p. 4 e.v. Het Cbp refereert in het advies aan artikel 11.3a Telecommunicatiewet. In het huidige wetsvoorstel betreft het artikel 11.7a Telecommunicatiewet.

98 Kamerstukken II 2010-2011, 32549, nr. 3, p. 79 e.v.

99 Groep Gegevensbescherming Artikel 29-2010 (I), p. 10.

100 Groep Gegevensbescherming Artikel 29-2010 (I), p. 11.

these conditions for some explicitly identified on-line services, always in the light of the general conditions of the Data Protection Directive"[101] en "The requirements for consent to be valid within Directive 2002/58/EC are the same as under Directive 95/46/EC".[102] In het licht van het voorgaande kan worden geconcludeerd dat de Wbp onverkort van toepassing is op artikel 11.7a Telecommunicatiewet. Dit betekent dat de betrokkene op grond van de artikelen 33 en 34 Wbp geïnformeerd dient te worden indien de verantwoordelijke cookies wil plaatsen en uitlezen.

2.2.3 Evaluatiestudies, onderzoeksrapporten en kabinetsstandpunten

In december 2007 presenteerden Zwenne et al. de onderzoeksresultaten van de eerste fase van de evaluatie van de Wbp. In deze literatuurstudie is geïnventariseerd in hoeverre en op welke wijze de Wbp een bijdrage heeft geleverd aan het realiseren van de doelstellingen van deze wet, alsmede welke knelpunten zich in de praktijk hebben voorgedaan bij de uitvoering en toepassing daarvan. Wat betreft de informatieplicht merken de auteurs op dat de open normen bij verantwoordelijken rechtsonzekerheid teweegbrengen over hetgeen de betreffende bepalingen hier concreet vereisen, en dat deze rechtsonzekerheid omtrent de inhoud en omvang van de informatieplicht ook onnodige uitvoeringskosten met zich meebrengt.[103] Voorts stellen Zwenne et al. met betrekking tot de informatieplicht het volgende:

(i) De open normen leiden tot interpretatiemoeilijkheden:

> "De informatieplicht is vervat in een norm die met veel open begrippen is geformuleerd, wat tot interpretatiemoeilijkheden leidt." [104]

(ii) De informatieplicht is bij weinig verantwoordelijken bekend:

> "Bij het algemene publiek lijkt de Wbp weinig bekend; met de bekendheid van de rechten en plichten die voortvloeien uit de Wbp is het niet veel beter gesteld. Die bekendheid met materiële rechten en plichten is natuurlijk belangrijker dan de kennis van het bestaan van een wet. Toch blijkt dat juist een in het oog springende norm als de informatieplicht (ook als die wordt uitgelegd naar z'n materiële inhoud) uit de Wbp bij weinig verantwoordelijken bekend is."[105]

---

101 Groep Gegevensbescherming Artikel 29-2011, p. 11.

102 Groep Gegevensbescherming Artikel 29-2011, p. 34. Zie in dit kader ook TNO/IViR, p. 14 en Zuiderveen Borgesius, p. 217.

103 Zwenne et al., p. 106.

104 Zwenne et al., p. 170.

105 Zwenne et al., p. 171.

(iii) De informatieplicht wordt door de verantwoordelijke te generiek ingevuld. Dit is ten dele te wijten aan de Wbp, maar ook aan het gemis aan concretisering van normen via lagere regelgeving en het ontbreken van jurisprudentie:

> "Van de informatieplicht van de verantwoordelijke richting betrokkene wordt geconstateerd dat deze vaak in te algemene zin wordt ingevuld: de doeleinden van de verwerking lenen zich bijvoorbeeld, net als bij de meldingsplicht, voor een generieke invulling. De onbekendheid van het instrumentarium van de Wbp kan niet aan de wet zelf worden geweten; voor de moeilijkheden bij de toepassing van de bepalingen omtrent rechten en plichten moet ten dele naar de wet, en ten dele naar het gebrek aan invulling van normen in lagere regelgeving en in de rechtspraak worden verwezen."[106]

In vervolg op de literatuurstudie hebben Winter et al. empirisch onderzoek verricht naar de werking van de Wbp. De probleemstelling van dit onderzoek luidde: *In hoeverre voldoet de werking van de Wbp in de praktijk aan de doelstellingen van de wet, in het bijzonder gelet op de in de literatuur gesignaleerde knelpunten en welke aanpassingen zijn mogelijk en wenselijk binnen het kader van de EU-richtlijn?* [107]

Het empirisch onderzoek werd bij de navolgende (deel)populaties uitgevoerd:[108]

1. Organisaties in het algemeen.
2. Meldende organisaties. Met deze groep worden die organisaties bedoeld die ten minste één melding bij het Cbp hebben gedaan.
3. Organisaties met een Functionaris voor de Gegevensbescherming.

Met betrekking tot de informatieplicht formuleerden Winter et al. de navolgende deelvraag: *Hoe is de naleving van de informatieplicht en leidt dat er toe dat de burger regie voert over zijn gegevens?*[109] De uitkomsten lieten zien dat in 72 procent van de gevallen organisaties in het algemeen de betrokkenen informeren over de gegevensverwerking. Driekwart van de meldende organisaties informeert de betrokkenen over de gegevensverwerking.[110] In de gevallen waarin dat niet gebeurt, is de hoofdreden dat de verantwoordelijke van mening is dat de betrokkene al op de hoogte is van de verwerking, bijvoorbeeld omdat deze zijn gegevens zelf beschikbaar heeft gesteld.[111] Winter et al. geven geen inzicht in het percentage organisaties dat een Functionaris voor de Gegevensbescherming heeft, en waar

---

106 Zwenne et al., p. 171.

107 Winter et al., p. 15.

108 Voor een nadere omschrijving van de onderzochte (deel)populaties en de keuzes die hieraan ten grondslag liggen wordt verwezen naar Winter et al., p. 53 e.v.

109 Winter et al., p. 18.

110 Winter et al., p. 80.

111 Winter et al., p. 89.

de betrokkenen geïnformeerd worden over het feit dat hun persoonsgegevens worden verwerkt.[112]

Een tweede conclusie uit het onderzoek laat zien dat de meeste respondenten van oordeel zijn dat de betrokkenen goed door hen worden geïnformeerd.[113] Dit is opmerkelijk aangezien in de literatuurstudie met betrekking tot de informatieplicht de deelconclusies werden getrokken dat (i) de open normen in relatie tot de informatieplicht tot interpretatieproblemen leiden, (ii) de informatieplicht bij weinig verantwoordelijken bekend is en (iii) de informatieplicht door de verantwoordelijke te generiek wordt ingevuld.[114] Met betrekking tot de open normen uit de Wbp stellen Winter et al. dat het een knelpunt wordt als blijkt dat nadere normering door middel van gedragscodes en regelingen per branche of sector niet tot ontwikkeling komt.[115]

Ook uit eerder uitgevoerd empirisch onderzoek van TNS NIPO onder huisartsen, onderwijsinstellingen en woningcorporaties volgt dat de informatieplicht veelal niet of niet juist wordt nageleefd.

> "De uitkomsten van het onderzoek suggereren dat ongeveer de helft van de huisartsen voldoet aan de informatieplicht."[116]

> "Op basis van de uitkomsten van het onderzoek schatten we dat ongeveer tweederde van de onderwijsinstellingen de informatieplicht naleeft maar dat niet helemaal juist doet."[117]

> "Op basis van de resultaten van het onderzoek schatten we in dat ongeveer de helft van de woningcorporaties de informatieplicht naleeft maar dat niet helemaal juist doet."[118]

Daarbij dient te worden aangetekend dat in het TNS NIPO onderzoek de reikwijdte van de informatieplicht uit de Wbp lijkt te zijn beperkt tot het verschaffen van informatie over de identiteit (de naam, het adres en de plaats) van de organisatie die de persoonsgegevens verwerkt en het doel van de gegevensverwerking.[119]

---

112 Een dergelijk inzicht zou voor dit onderzoek wenselijk zijn geweest, aangezien op basis hiervan wellicht een aanwijzing zou kunnen worden gevonden over een mogelijke relatie tussen zelfregulering en de naleving van de informatieplicht.

113 Winter et al., p. 89.

114 Zwenne et al., p. 170 e.v.

115 Winter et al., p. 157.

116 TNS NIPO, p. 13.

117 TNS NIPO, p. 23.

118 TNS NIPO, p. 32.

119 TNS NIPO, p. 1.

Een mogelijke reden voor de tegenstelling in de uitkomsten van het onderzoek van Zwenne et al. en TNO NIPO enerzijds en Winter et al. anderzijds is wellicht gelegen in het feit dat het responsepercentage in het empirisch onderzoek onder de organisaties gemiddeld slechts 13 procent was.[120] Bovendien merken Winter et al. met betrekking tot de organisaties op dat de verdeling van respondenten over typen organisaties en aantallen werknemers tot gevolg heeft dat de uitspraken op basis van de enquête in het algemeen weinig zicht geven op het totaalbeeld van de dagelijkse praktijk bij verwerkende organisaties in Nederland. “De enquête geeft dan ook geen representatief beeld, maar laat een topje van de ijsberg zien. Dat betekent dat de resultaten informatief kunnen zijn als indicatie voor bijvoorbeeld beweegredenen van bepaalde acties, maar dat er geen absolute waarde aan kan worden toegekend”, aldus Winter et al.[121] Tenslotte wijzen de onderzoekers op het feit dat het lastig is gebleken een goede respons op de enquête te krijgen. “Als we het hebben over de uitvoering van de Wbp, dan geeft deze groep het beste beeld hoe deze wet ‘gemiddeld’ wordt uitgevoerd. Dit kan een sterke tegenstelling vormen met de (juridische) literatuur en het eerste faseonderzoek, die meer focussen op grote, belangrijke en wellicht ook atypische zaken”.[122] Ook het feit dat voornoemde onderzoeken niet dezelfde populaties bestreken, kan wellicht het geconstateerde verschil in uitkomst verklaren.

Eind 2007 is op initiatief van de minister van Justitie en de minister van Binnenlandse Zaken en Koninkrijksrelaties de Adviescommissie Veiligheid en persoonlijke levenssfeer, onder voorzitterschap van Brouwer-Korf, ingesteld.[123] Een belangrijke aanleiding voor het instellen van deze adviescommissie vormde het beleidsprogramma ‘Samen werken, samen leven’ van het kabinet Balkenende IV, waarin was bepaald dat bij de aanpak van agressie, geweld en criminaliteit het kabinet privacybelemmeringen voor betrokken beroepsgroepen aanpakt en onderzoek naar en ontwikkeling van preventieprogramma’s stimuleert.[124] Overigens had het kabinet ook de behoefte aan een advies over de wijze waarop de veiligheid ten goede kan komen aan de persoonlijke levenssfeer en vice versa. De Commissie Brouwer-Korf werd kortom gevraagd te adviseren over de regulering van, voorlichting over, werkwijzen bij en indien nodig protocollisering van de omgang met persoonsgegevens, zodat deze de veiligheid van personen bevorderen.[125] In het eindrapport wijst de Commissie in het kader van de informatieplicht op het ontstaan van ‘slimme omgevingen’, waarbij de technologie steeds meer wordt verweven met de omgeving. Een dergelijk slimme omgeving wordt naar de mening van de Commissie gekenmerkt door een onzichtbaar netwerk van intelligente

120 Winter et al., p. 56.

121 Winter et al., p. 57.

122 Winter et al., p. 54.

123 Besluit instelling Adviescommissie Veiligheid en persoonlijke levenssfeer d.d. 19 december 2007. Deze regeling is vervallen op 1 januari 2009.

124 Beleidsprogramma Samen werken, samen leven, onder pijler V (Veiligheid, stabiliteit en respect).

125 Besluit instelling Adviescommissie Veiligheid en persoonlijke levenssfeer d.d. 19 december 2007, Toelichting onder punt 1.

computers, sensoren en andere ICT-middelen, ofwel er ontstaat een intelligente, onzichtbare ICT-infrastructuur die anticipeert en reageert op personen die zich in de omgeving bevinden. De Commissie merkt bovendien op dat, naarmate de toepassing van dit soort technologieën toeneemt, het steeds moeilijker wordt voor individuen om zich hieraan te onttrekken. In dat kader komt ze tot de conclusie dat de informatieplicht uit de Wbp niet langer een voldoende waarborg kan bieden, met als gevolg dat er slechts zicht bestaat op wat er in eerste instantie met de gegevens gebeurt maar niet wat een volgende organisatie ermee doet.[126] Ogenschijnlijk heeft de Commissie geen vertrouwen in de werking van artikel 34 Wbp, gezien de stelling dat op grond van de informatieplicht uit de Wbp slechts zicht wordt verkregen op hetgeen in eerste instantie gebeurt met persoonsgegevens, en dat daarna het traject van gegevensverwerking klaarblijkelijk ondoorzichtig wordt, althans niet zichtbaar en inzichtelijk gemaakt kan worden met behulp van de informatieplicht uit de Wbp. De Commissie impliceert daarmee dat de overheid en het bedrijfsleven onvoldoende invulling geven aan artikel 34 lid 1 sub a Wbp. Op grond van dit artikel dienen immers 'ontvangers in tweede instantie' de betrokkene te informeren op het moment van vastlegging van hem betreffende persoonsgegevens. De Commissie meent dat transparantie steeds belangrijker wordt, omdat alleen zo burgers nog zicht houden op het gebruik van hun gegevens door overheid en bedrijfsleven. 'Transparantie, tenzij'[127] is dan ook één van de zes grondslagen die in het eindrapport wordt gedefinieerd in een richtinggevend kader voor informatieverwerking en veiligheid. Dit kader beoogt bij te dragen aan rationaliteit en consistentie bij beslissingen waar spanning kan ontstaan tussen veiligheid en persoonlijke levenssfeer.[128]

> "Het richtinggevend kader omvat naast grondslagen tevens handreikingen die algemeen zijn toe te passen bij de afwegingen tussen veiligheid en privacy. De grondslagen luiden als volgt:
> 1. Transparantie, tenzij;
> 2. Selecteer voor je verzamelt en houd het sober;
> 3. Indien noodzakelijk voor de veiligheid, moet je delen;
> 4. Zorg voor integriteit van gegevens, systemen en het handelen van gebruikers;
> 5. Zorg voor voorlichting en faciliteiten;
> 6. Zorg voor naleving en intern toezicht." [129]

---

126 Brouwer-Korf, p. 28.

127 Met 'tenzij' wordt bedoeld dat er ruimte is voor uitzonderingen. "Een zeer beperkte ruimte, die eigenlijk alleen benut kan worden in evidente situaties: bijvoorbeeld bij het werk van inlichtingen- en veiligheidsdiensten of in het kader van een strafrechtelijk onderzoek. En ook zou het onwerkbaar worden wanneer nooit een beleidsverandering doorgevoerd zou kunnen worden zonder toestemming van alle mensen van wie persoonsgegevens verzameld zijn". Brouwer-Korf, p. 47.

128 Brouwer-Korf, p. 3.

129 Brouwer-Korf, p. 42 e.v.

In de ogen van de Commissie impliceert transparantie dat het voor de betrokkene duidelijk moet zijn wie zijn gegevens verzamelt, met welk doel zijn gegevens worden verzameld en wat er vervolgens met zijn gegevens gebeurt. Daarnaast merkt de Commissie op dat transparantie zowel een generiek als een specifiek aspect kent, waarbij aan beide aspecten dient te worden voldaan. Het generieke aspect impliceert dat actief dient te worden gecommuniceerd over met name doelstelling, middelen, proportionaliteit en subsidiariteit van een systeem voor het omgaan met persoonsgegevens. De Commissie benadrukt dat juist op het moment van verzamelen het belangrijk en noodzakelijk is de burger te informeren over het doel van de verzameling en het gebruik, zoals beoogd op het moment van het verzamelen van gegevens. Het specifieke aspect impliceert dat degene wiens gegevens actief worden verwerkt wordt geïnformeerd over de doelstellingen van de verwerking, welke gegevens het betreft, met welke instanties voor welk doel wordt uitgewisseld en dient de betrokkene te worden gewezen op diens rechten en verplichtingen.[130]

Bij brief van de minister van Justitie en de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer bood het kabinet het standpunt aan inzake zowel de bevindingen van de Commissie Brouwer-Korf als de Wbp-evaluatierapporten.[131] In de inleiding benadrukt het kabinet dat de verwerking en de bescherming van persoonsgegevens van vitaal belang zijn voor het functioneren van de hedendaagse samenleving. Tevens wijst het kabinet erop dat ten gevolge van de ontwikkeling van technologie persoonsgegevens gemakkelijker kunnen worden verspreid en gedeeld, maar ook dat in toenemende mate gegevens over burgers worden vastgelegd, zowel in de publieke als in de private sector. Breder gebruik stelt hogere eisen aan de kwaliteit en aan de beveiliging van gegevens, om fouten en misbruik te voorkomen, aldus de kabinetsreactie.[132] In navolging van de Commissie Brouwer-Korf onderschrijft het kabinet Balkenende IV het belang van transparantie. Het kabinet wijst erop dat juist de transparantie in de huidige samenleving in toenemende mate onder druk lijkt te staan, en dat niet voorbij kan worden gegaan aan het feit dat het aantal databanken waarin gegevens van burgers zijn opgeslagen is toegenomen. Dat verschijnsel is onvermijdelijk verbonden aan de informatiesamenleving, aldus het kabinet.[133] Tevens stelt het kabinet dat, wat betreft de wijze waarop transparantie wordt vormgegeven, het veiligheidsdomein afwijkt van de andere domeinen aangezien het niet altijd in het belang is van de veiligheid om volledige transparantie te bieden. Naar de mening van het kabinet dient, in geval van het ontbreken van volledige transparantie, de burger gecompenseerd te worden met andere middelen zoals toezicht door één of soms meer instanties en door middel van toetsing door de rechter

130 Brouwer-Korf, p. 45.
131 Kamerstukken II 2009–2010, 31051, nr. 5.
132 Kamerstukken II 2009–2010, 31051, nr. 5, p. 3.
133 Kamerstukken II 2009–2010, 31051, nr. 5, p. 22.

achteraf.[134] Wat betreft het richtinggevend kader dat de Commissie Brouwer-Korf presenteerde merkt het kabinet op dat deze zonder verdere uitwerking zowel krachtig als kwetsbaar is. De grondslagen zijn weliswaar breed toepasbaar, maar bieden zonder nadere sectorale uitwerking nog geen garantie voor zorgvuldige afwegingen door professionals.[135] Daarbij tekent het kabinet aan dat de verwerking van persoonsgegevens voornamelijk plaats vindt buiten het veiligheidsdomein en is het kabinet van mening dat in dit kader de Wbp van groot belang is. In relatie tot het door het kabinet gedefinieerde kernthema burgerperspectief[136] en het door het kabinet onderschreven belang van transparantie, wordt opgemerkt dat een voldoende mate van transparantie naar burgers toe over wat er met hun gegevens gebeurt, een noodzakelijke voorwaarde is voor een sterkere en bewustere burger. Naar de mening van het kabinet kan een burger pas keuzes maken wanneer hij ook daadwerkelijk weet voor welk doel zijn gegevens worden verwerkt, met welke andere gegevens die gegevens in verband worden gebracht en vervolgens aan anderen ter beschikking worden gesteld, waar ze beschikbaar zijn en hoe het inzage- en correctierecht kan worden uitgeoefend.[137] Het kabinet wijst op dit punt naar het rapport Regioplan waarin wordt gesteld dat controle en transparantie wezenlijk zijn voor acceptatie van gegevensverwerking door burgers.[138] Het kabinet wil derhalve dat de betrokkene wordt geïnformeerd door de verantwoordelijke. Nu bestaat deze verplichting reeds op grond van artikel 33 en 34 Wbp, maar schijnbaar is het kabinet van mening dat de informatieplicht onvoldoende door de verantwoordelijke wordt nagekomen. Het kabinet laat, naast het willen versterken van de handhavingstaak van het Cbp, voor het overige in het midden welke concrete maatregelen worden overwogen ter bevordering van de naleving van de informatieplicht. Wel overweegt het kabinet om de informatieplicht uit te breiden door de verantwoordelijke te verplichten om de betrokkene inzicht te geven in eventuele categoriseringen die plaatsvinden op basis van verzamelde persoonsgegevens en de daartoe achterliggende redenen.[139]

Op 3 februari 2010 vond overleg plaats tussen de vaste kamer commissies voor Justitie en voor Binnenlandse Zaken en Koninkrijksrelaties en de ministers van Justitie en Binnenlandse Zaken en Koninkrijksrelaties over zowel de Wbp-evaluaties als het voornoemde kabinetsstandpunt.[140] De algemene teneur van de leden van de commissies met betrekking tot de door het kabinet bepleite transparantie is dat zij onderstrepen dat de burger moet weten welke gegevens over hem zijn opgeslagen, wie er iets mee doet en wat

134 Kamerstukken II 2009–2010, 31051, nr. 5, p. 13.
135 Kamerstukken II 2009–2010, 31051, nr. 5, p. 11.
136 Kamerstukken II 2009–2010, 31051, nr. 5, p. 7.
137 Kamerstukken II 2009–2010, 31051, nr. 5, p. 22.
138 Regioplan, p. 44.
139 Kamerstukken II 2009–2010, 31051, nr. 5, p. 23.
140 Kamerstukken II 2009–2010, 31051, nr. 7.

er mee wordt gedaan. Zij vragen zich echter af wat er in de praktijk moet gebeuren om die transparantie te creëren en welke maatregelen het kabinet daartoe wil gaan nemen aangezien in het kabinetsstandpunt daar slechts op hoofdlijnen wordt ingegaan.

> SP-fractie: “Veel mensen vinden het helemaal niet erg wanneer veel gegevens over hen zijn opgeslagen, zolang er maar zorgvuldig wordt omgegaan met hun informatie. Mensen moeten weten welke gegevens over hen zijn opgeslagen, wie er iets mee doet en wat er mee wordt gedaan. Het moet volstrekt helder zijn wat er met hun gegevens gebeurt en hoe zij tegen eventueel misbruik zijn beschermd. Dat schrijft de minister allemaal wel, maar hij verbindt er geen gevolgen aan. Wij vinden dat de burger veel beter dan nu moet worden geïnformeerd over het verwerken van persoonsgegevens door bedrijven en de overheid. Als je niet weet wie welke informatie heeft, kun je ook je rechten niet goed uitoefenen. De rechten op dit gebied moeten worden versterkt. Het recht op informatie en inzage en het recht op correctie of verwijdering van gegevens zijn in de wet geregeld, maar wat gebeurt er in de praktijk als mensen niet weten dat zij die rechten hebben? De commissie Brouwer-Korf benadrukt de transparantie en daarin kan ik mij vinden, maar wat gaan wij in de praktijk doen? Wat gaat de minister doen om de rechten in de praktijk sterker te maken en dan niet alleen op papier?”[141]

> VVD-fractie: “De VVD-fractie is met het kabinet van mening dat burgers zich bewuster moeten zijn van het vrijgeven van hun gegevens en het daarmee gepaard gaande opgeven of benadelen van hun eigen privacy. Met de grondslagen die de commissie noemt, zoals de transparantie tenzij, select before you collect, bij veiligheid delen, integriteit van systemen en voorlichting en facilitering, zijn wij het van harte eens.”[142]

> PvdA-fractie: “De burger moet weten wanneer hij te maken heeft met het opslaan van zijn persoonsgegevens, wat het doel daarvan is en waarom het in die gevallen noodzakelijk is.”[143]

> Groen Links-fractie: “Het is van groot belang dat de burger precies weet wat waar wordt opgeslagen en hoe dat gebeurt.”[144]

> D66-fractie: “Naast de eigen verantwoordelijkheid van mensen voor wat zij zelf met hun gegevens doen, is meer transparantie nodig. Wat gaat het kabinet doen om de overheid

141 Kamerstukken II 2009–2010, 31051, nr. 7, p. 3.
142 Kamerstukken II 2009–2010, 31051, nr. 7, p. 6.
143 Kamerstukken II 2009–2010, 31051, nr. 7, p. 9.
144 Kamerstukken II 2009–2010, 31051, nr. 7, p. 12.

zelf transparanter te maken? Ik kijk uit naar de aangekondigde wetsvoorstellen om de transparantie te vergroten."[145]

In zijn antwoord stelt de minister van Justitie dat burgers zich beschermd moeten weten en het daarmee een kwestie is van vertrouwen in de overheid. Daarbij zijn vragen aan de orde als 'hoe de burgers beter geïnformeerd kunnen worden, waar zij zijn geregistreerd en hoe de klachtenregeling kan worden geoptimaliseerd', aldus de minister, waarbij hij refereert aan het rapport van de Commissie Brouwer-Korf waarin wordt opgemerkt dat het de taak van de organisaties zelf is om hun professionals daartoe voldoende toe te rusten. Voorts verduidelijkt de minister dat de overheid de professional ondersteunt met een helpdesk en dat het bedrijfsleven gestimuleerd moet worden om een goed privacybeleid te voeren.[146] Op welke wijze de overheid die stimulans wil creëren maakt de minister van Justitie op dat moment niet duidelijk, behalve door te stellen dat hij de handhavingstaak van het Cbp beoogd te versterken.[147]

Evenals de Tweede Kamer heeft ook de Eerste Kamer vragen gesteld als reactie op het kabinetsstandpunt.[148] Met betrekking tot de informatieplicht merkt de fractie van GroenLinks op dat de regering de informatieplicht wil verbeteren door middel van maatregelen bij de overheid, en stelt vervolgens de vraag of ook het bedrijfsleven moet worden verplicht tot betere informatieverstrekking aan klanten. Daarbij plaatst de fractie de kanttekening dat ze de informatieplicht onderschrijft, maar dat het toch nog steeds de omgekeerde wereld lijkt omdat burgers er zelf achteraan moeten gaan om te weten te komen wat er met hun gegevens gebeurt. De fractie stelt vervolgens de vraag of de overheid en het bedrijfsleven een burger, bij de verstrekking van persoonsgegevens, niet meteen op de hoogte moeten stellen van de mogelijke verwerking van zijn of haar gegevens, en hoe die verwerking te volgen is.[149] Als antwoord verwijst de minister van Justitie in minimale bewoording naar de informatieplicht zoals die voortvloeit uit de artikelen 33 en 34 Wbp, en waarin wordt voorgeschreven dat de burger actief geïnformeerd dient te worden bij doorgifte van gegevens aan derden.[150] De VVD-fractie stelt in het kader van de door het kabinet beoogde transparantie dat de burger door overheidsinstellingen en bedrijven die zijn gegevens verwerken beter moet worden geïnformeerd, en legt de vraag neer welke concrete maatregelen de overheid gaat treffen om die transparantie richting de burger te vergroten.[151] De minister van Justitie gaat in zijn antwoord slechts in op het persoonsinformatiebeleid ten

145 Kamerstukken II 2009–2010, 31051, nr. 7, p. 16.
146 Kamerstukken II 2009–2010, 31051, nr. 7, p. 19.
147 Kamerstukken II 2009–2010, 31051, nr. 7, p. 19.
148 Kamerstukken I 2009-2010, 31051, A.
149 Kamerstukken I 2009-2010, 31051, A, p. 7.
150 Kamerstukken I 2009-2010, 31051, A, p. 29.
151 Kamerstukken I 2009-2010, 31051, A, p. 16.

aanzien van de opslag en verwerking van persoonsgegevens in de publieke sector. “Dit beleid richt zich op het gebruik van persoonsgegevens bij dienstverlening en de uitvoering van taken in de publieke sector waarbij het doel is zorgvuldig om te gaan met persoonsgegevens van de burger en te komen tot een efficiënte inrichting van overheidsorganisaties waarbij de burger zo optimaal mogelijk wordt bediend”.[152] De leden van de fractie van D66 constateren naar aanleiding van het rapport van de Commissie Brouwer-Korf dat er geen specifieke verplichtingen bestaan om informatie over de gebruikswijzen van persoonsgegevens te verschaffen. Volgens de D66-fractie doet dat af aan de werking van de transparantieverplichting, en de fractie vraagt derhalve of het kabinet voornemens is een dergelijke voorziening op te nemen in de Wbp.[153] De minister van Justitie bevestigt dat de Wbp geen specifieke verplichtingen voor verantwoordelijken bevat om inzicht te geven aan alle varianten van het gebruik van verzamelde persoonsgegevens. “Wel bevat artikel 33, derde lid, van de Wbp de verplichting voor de verantwoordelijke om, met inachtneming van de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, zodanige nadere informatie te verschaffen aan de betrokkene dat een behoorlijke en zorgvuldige verwerking ten opzichte van hem gewaarborgd is”, aldus de minister van Justitie. Naar zijn mening is dit een voorschrift dat, wanneer goed nageleefd, een redelijke last op de verantwoordelijke legt en waaraan de betrokkene de nodige houvast kan ontlenen.[154]

In reactie op het rapport van de Commissie Brouwer-Korf stelt het Cbp dat het zich goed kan vinden in het richtinggevende kader dat in hoge mate spoort met de principes en bepalingen uit de Wbp. Daarenboven meent het Cbp dat het oordeel van de Commissie, dat transparantie cruciaal is voor een samenleving van vertrouwen, des te klemmender is omdat uit onderzoek is gebleken dat het aantal gegevensbestanden waarin burgers staan geregistreerd schrikbarend hoog is.[155] In het jaarverslag 2009 benadrukt het Cbp dat burgers moeten weten wie, waarom, waar en welke gegevens over hen verzamelt en gebruikt wordt, en stelt voorts dat de problemen bij de bescherming van persoonsgegevens in de private sector onder meer zijn te wijten aan het feit dat bedrijven de burger niet voldoende informeren over het gebruik van zijn persoonsgegevens noch over de verstrekking van zijn gegevens aan derden. Eén van de door het Cbp gedefinieerde speerpunten voor 2010 is dan ook om te onderzoeken in welke mate en op welke wijze bedrijven aan hun verplichtingen voldoen om burgers te informeren, alsook zal het Cbp doen overgaan tot het opstellen van Richtsnoeren inzake de informatieplicht.[156]

---

152 Kamerstukken I 2009-2010, 31051, A, p. 43.

153 Kamerstukken I 2009-2010, 31051, A, p. 16.

154 Kamerstukken I 2009-2010, 31051, A, p. 44.

155 Cbp, Persverklaring 22 januari 2009.

156 Cbp Jaarverslag 2009, p. 10. Deze door het Cbp aangekondigde richtsnoeren waren ten tijde van het afsluiten van dit onderzoek nog niet gepubliceerd.

In de literatuur zijn kanttekeningen geplaatst bij het rapport van de Commissie Brouwer-Korf en het standpunt van het kabinet. Dommering merkt op dat het rapport de bijl zet in het kernbeginsel van het privacyrecht, de doelbinding, die slechts in concreet af te wegen gevallen mag wijken voor belangen van een andere orde. “Het rapport formuleert als hoofdbeginsel zonder nadere concrete belangenafweging: ‘indien noodzakelijk voor de veiligheid, moet je delen.’ Dit is niet een ‘verzoening’ van privacy en veiligheid (de taak van de Commissie), maar een onderschikking van privacy aan veiligheid”.[157] Met betrekking tot het kabinetsstandpunt is Duthler van mening dat het juridisch denken dominant is, en merkt zij op dat veel voornemens van het kabinet gericht zijn op nieuwe wetgeving. Zij stelt in dat kader dat privacybescherming echter meer is dan het toepassen van regels, en dat het juist ook gaat om het implementeren van uitgangspunten en regels in systemen, organisaties, in procedures en maatregelen.[158] Wat betreft het standpunt van het kabinet dat burgers door overheidsinstellingen en bedrijven die hun gegevens verwerken beter moeten worden geïnformeerd, merkt Duthler op dat het kabinet zich niet uitlaat over concrete maatregelen die de overheid gaat treffen om die transparantie voor de burger te vergroten.[159] Naar de opvatting van Buitelaar en Cuijpers is de kabinetsreactie primair procedureel van aard, en kenmerkt het zich door veel herhaling en een vrijwel uitputtende tour d’horizon van de verschillende rapporten, evaluaties en expert group meetings die de afgelopen periode zijn verschenen.[160] Met betrekking tot de door het kabinet aangehaalde waarborgen die gelden voor de privacy van burgers in relatie tot het delen van informatie tussen overheidsorganisaties, evenals andere waarborgen waaraan op diverse plaatsen in het kabinetsstandpunt aandacht wordt geschonken, merken Buitelaar en Cuijpers op dat het kabinet oppervlakkig blijft wat deze waarborgen precies inhouden, en in hoeverre deze anders zijn of verder gaan dan de waarborgen die nu reeds verankerd liggen in de huidige wetgeving. Tevens plaatsen Buitelaar en Cuijpers kanttekeningen bij de rol die het kabinet toedeelt aan de professionals die in de praktijk de afweging moeten maken tussen veiligheid en privacy, de door het kabinet voorgestelde maatregelen ter zake klachtenbehandeling, de mogelijk veranderende positie van de functionaris gegevensbescherming en de wijze waarop het kabinet al dan niet tegemoet komt aan de privacybeleving van de burgers.[161] Buitelaar en Cuijpers komen tot de slotconclusie dat de komende tijd de ontwikkelingen op het privacyterrein dienen te worden gevolgd, aangezien veel van de actiepunten die in het kabinetsstandpunt naar voren worden gebracht nadere wettelijke inkadering behoeven dan wel uitgewerkt en uitgevoerd moeten worden. Voorts menen zij dat op basis van de kabinetsreactie vooralsnog slechts gehoopt, maar nog niet verwacht, kan worden dat een

157 Dommering 2010, p. 87.
158 Duthler, p. 59 e.v.
159 Duthler, p. 61.
160 Buitelaar & Cuijpers, p. 2820.
161 Voor de inhoud van deze kanttekeningen verwijs ik naar Buitelaar & Cuijpers.

maatschappelijke acceptabele balans tussen veiligheid en privacy daadwerkelijk tot stand zal komen.[162]

Op 30 september 2010 is het kabinet Rutte aangetreden. In het regeerakkoord wordt door het kabinet op hoofdlijnen enkele maatregelen en voorstellen aangekondigd ter verbetering van de bescherming van persoonsgegevens.[163] Eind december 2010 heeft het kabinet meer inhoudelijke standpunten kenbaar gemaakt ten aanzien van de bescherming van persoonsgegevens.[164] De aanleiding hiervoor is gelegen in de evaluatie van de Privacyrichtlijn. Deze evaluatie heeft geresulteerd in een mededeling van de Europese Commissie waarin de aanpak uiteen wordt gezet met het oog op de modernisering van de wettelijke regeling van de EU voor de bescherming van persoonsgegevens.[165] Een hoofddoelstelling in het raamwerk betreft het versterken van de rechten van individuen. In dat kader expliciteert de Commissie dat de bestaande bepalingen betreffende de aan de betrokkene te verstrekken informatie niet toereikend zijn.[166] De Europese Commissie is van mening dat transparantie een basisvoorwaarde is, willen individuen controle kunnen uitoefenen over hun eigen gegevens en zich van een effectieve bescherming van hun persoonsgegevens kunnen verzekeren. “Het is van wezenlijk belang dat individuen door degenen die voor de verwerking verantwoordelijk zijn goed en duidelijk, op een transparante wijze, worden geïnformeerd over hoe en door wie hun gegevens worden verzameld en verwerkt, voor welke doeleinden, gedurende welke periode en in hoeverre zij het recht hebben hun gegevens in te zien, te corrigeren of te wissen”.[167] De Commissie heeft daarom in 2010 aangekondigd een algemeen beginsel van transparante verwerking van persoonsgegevens op te willen nemen in de herziene Privacyrichtlijn.[168] Tevens zal de Europese Commissie de mogelijkheden onderzoeken om de praktische regelingen voor de feitelijke uitoefening van het recht op inzage, correctie, verwijdering of afscherming van gegevens te verbeteren.[169] In reactie op de mededeling van de Europese Commissie stelt het kabinet Rutte zich op het standpunt dat er geen noodzaak is de algemene formulering van de transparantieverplichting zoals bepaald in de artikelen 33 en 34 Wbp te herzien.[170] Ook de voorwaarden voor de uitoefening van de rechten van inzage, correctie en verzet behoeven volgens het kabinet op zichzelf genomen geen herziening.[171] In dezelfde reactie

162 Buitelaar & Cuijpers, p. 2825.
163 Regeerakkoord VVD-CDA, Vrijheid en verantwoordelijkheid, d.d. 30 september 2010, p. 42.
164 Kamerstukken II 2010-2011, 22122, nr. 1116.
165 COM (2010) 609 definitief.
166 COM (2010) 609 definitief, p. 6 e.v. Vergelijk Brouwer-Korf die tot de conclusie komt dat de informatieplicht uit de Wbp niet langer een voldoende waarborg kan bieden. Brouwer-Korf, p. 28.
167 COM (2010) 609 definitief, p. 6 e.v.
168 COM (2010) 609 definitief, p. 6.
169 COM (2010) 609 definitief, p. 9.
170 Kamerstukken II 2010-2011, 22122, nr. 1116, p. 4.
171 Kamerstukken II 2010-2011, 22122, nr. 1116, p. 5.

wordt door het kabinet aangekondigd dat op korte termijn een nadere visie op privacy zal worden gepresenteerd.[172] De leden van de vaste commissie Veiligheid en Justitie en de commissie Binnenlandse Zaken van de Eerste Kamer hebben vooruitlopend op het beleidsdebat over de visie van het kabinet diverse vragen gesteld.[173] Deze zijn op 29 april 2011 door de minister van Binnenlandse Zaken en Koninkrijksrelaties en de staatssecretaris beantwoord.[174] In de beantwoording van de vragen rondom de transparantieverplichtingen wordt verwezen naar de maatregelen die het kabinet beoogt aan te kondigen. Het kabinet heeft haar visie op privacy uiteindelijk neergelegd in de Notitie Privacybeleid van 29 april 2011.[175] "De notitie ziet primair op de uitvoering van reeds gepresenteerde plannen in het regeerakkoord alsmede een aantal al eerder voorgenomen maatregelen".[176] Met betrekking tot de transparantieverplichting kondigt het kabinet aan in een voorstel tot wijziging van de Wbp de volgende voorzieningen ter versterking van de naleving van de Wbp op te nemen:

1. Een explicitering van de transparantieverplichting van de verantwoordelijke om vastgestelde bewaartermijnen bekend te maken en een mededelingsplicht van hetgeen met de verwerkte persoonsgegevens gebeurt na afloop van de termijn;[177] en
2. Een afzonderlijke regeling voorzien van specifieke transparantieverplichtingen bij het toepassen van profileringen, met inbegrip van een explicitering van het doel van de verwerking, en de daarbij gehanteerde categoriseringen.[178]

Tevens stelt het kabinet dat zij voorgenomen maatregelen op informatiegebied nadrukkelijker zal toetsen aan effectiviteit en transparantie, alsmede dat die maatregelen zullen worden voorzien van evaluatie- of horizonbepalingen.[179]

Hiervoor is gerefereerd aan de overweging van de Europese Commissie om een algemeen beginsel van transparantie inzake de verwerking van persoonsgegevens op te nemen in de herziene Privacyrichtlijn, en de afwijzende reactie hierop van het kabinet Rutte. De European Data Protection Supervisor (EDPS) daarentegen ondersteunt de overweging van de Europese Commissie: "According to the EDPS, it could have added value to include an *explicit* principle of transparency, either or not linked to the existing provision of fair processing. This would increase legal certainty and also confirm that a controller should under all circumstances process personal data in a transparent way, not only on request or when a specific legal provision requires him to do so".[180] Tevens stelt de EDPS voor om de huidige bepalingen van artikel 10 en 11 van de Richtlijn aan te scherpen. "However, it is

172 Kamerstukken II 2010-2011, 22122, nr. 1116, p. 3.
173 Kamerstukken II 2010-2011, 32761, nr. 1, blg-115091 (afschrift).
174 Kamerstukken II 2010-2011, 32761, nr. 1, blg-115089.
175 Kamerstukken II 2010-2011, 32761, nr. 1.
176 Kamerstukken II 2010-2011, 32761, nr. 1, p. 4.
177 Kamerstukken II 2010-2011, 32761, nr. 1, p. 1.
178 Kamerstukken II 2010-2011, 32761, nr. 1, p. 1.
179 Kamerstukken II 2010-2011, 32761, nr. 1, p. 2.
180 EDPS, p. 16.

perhaps more important to reinforce the existing provisions dealing with transparency, such as the existing Articles 10 and 11 of Directive 95/46. Those provisions specify the information elements that must be provided, but are not precise on the modalities. More concretely, the EDPS suggests strengthening the existing provisions by:

1. A requirement for a controller to provide information on data processing in a manner which is easily accessible and easy to understand, and in clear and plain language. The information should be clear, conspicuous and prominent. The provision could also encompass the obligation to ensure easy understanding of the information. This obligation would render illegal privacy policies which are opaque or difficult to understand.
2. A requirement to render the information easily and directly to data subjects. The information should also be permanently accessible, and not after a very short time disappear from an electronic medium. This would help users to store and reproduce information in the future, enabling further access". [181]

Eerder expliciteerde de Groep Gegevensbescherming Artikel 29 al dat, vanuit het oogpunt van transparantie, de artikelen 10 en 11 Privacyrichtlijn moeten worden herzien. "Transparency is another fundamental condition, as it gives the data subject a say in the processing of personal data, *'ex ante'*, prior to processing. Profiling, data mining, and technological developments which ease the exchangeability of personal data make it even more important for the data subject to be aware by whom, on what grounds, from where, for what purposes and with what technical means data are being processed. It is important that this information is understandable. However, the duty to inform the data subject (Articles 10 and 11 of Directive 95/46/EC) is not always properly put into practice. A new legal framework should provide alternative solutions, in order to enhance transparency".[182]

Uit het voorstel van de Europese Commissie (2012) lijkt te kunnen worden opgemaakt dat de Commissie het transparantiebeginsel daadwerkelijk meer expliciet dan voorheen wil introduceren.[183] Het beginsel zal, althans zo blijkt uit het voorstel, worden opgenomen in artikel 5 sub a.

> Article 5 Principles relating to personal data processing
> Personal data must be:
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

In de toelichting maakt de Commissie duidelijk dat het transparantiebeginsel een nieuw element is. "Article 5 sets out the principles relating to personal data processing, which correspond to those in Article 6 of Directive 95/46/EC. Additional new elements are in particular the transparency principle, the clarification of the data minimisation principle and

181 EDPS, p. 16 e.v.
182 Groep Gegevensbescherming Artikel 29-2009, p. 16.
183 COM (2012) 11 final.

the establishment of a comprehensive responsibility and liability of the controller".[184] Het standpunt van het kabinet Rutte dat een herziening van de artikelen 33 en 34 Wbp niet aan de orde is, lijkt daarmee van de ambities van de diverse Europese spelers af te wijken. Het onderwerp van een algemeen beginsel van transparante verwerking van persoonsgegevens is niet aan de orde gekomen gedurende de beleidsdebatten die de minister van Binnenlandse Zaken en Koninkrijksrelaties en de staatssecretaris van Veiligheid en Justitie hebben gevoerd met de vaste commissies van de Eerste en Tweede Kamer over de Notitie Privacybeleid. In het debat met de Eerste Kamer benadrukt de staatssecretaris dat "het kabinet zal komen met voorstellen om de algemene transparantieverplichtingen te preciseren en een specifieke transparantieverplichting te introduceren voor bijvoorbeeld het profilen".[185] Voorts stelt de staatssecretaris dat bedrijven en overheid transparantie moeten betrachten, en dat zij verzoeken om inzage en correctie, zeker als het verzoek om correctie een wijziging van onjuiste gegevens betreft, behoorlijk moeten behandelen.[186] Ook in het beleidsdebat tussen voornoemde bewindslieden en de vaste commissie van de Tweede Kamer van 15 september 2011, wordt niet of nauwelijks gerefereerd aan (ontwikkelingen ten aanzien van) de transparantieplicht.[187]

In de beleidsdebatten wordt door het kabinet benadrukt dat het met een visie zal komen met betrekking tot het rapport *i*Overheid van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). In dit rapport laat de WRR zien dat de overheid onder invloed van digitalisering fundamenteel van karakter verandert, waarbij samenhangende informatiestromen het karakter van de overheid domineren. De WRR concludeert vervolgens dat in de dagelijkse werkelijkheid van politiek en bestuur allesbehalve vanuit het samenhangende idee van deze informatie-Overheid – *iOverheid* – wordt gedacht en gewerkt.[188] Naar de mening van de WRR is er dan ook een inhoudelijke en institutionele transformatie nodig om de doelen voor de *i*Overheid handen en voeten te geven. De Raad onderscheidt wat betreft de institutionele transformatie een drietal functies, waarvan de maatschappelijke functie er een is.[189] Met deze functie wordt onder meer beoogd een veel grotere mate van openheid en transparantie richting burgers te realiseren om hen aldus meer en beter inzicht te bieden in de informatie die de *i*Overheid over hen heeft vergaard en hen tevens te faciliteren de informatie waar nodig te corrigeren. "Burgers staan nu vrijwel machteloos als zij persoonlijk worden geconfronteerd met fouten in de uitgestrekte informatienetwerken van de *i*Overheid die soms grote gevolgen hebben".[190] De WRR houdt

184 COM (2012) 11 final, p. 8.
185 Handelingen I 2010-2011, nr. 27, item 11, p. 53.
186 Handelingen I 2010-2011, nr. 27, item 11, p. 53.
187 Kamerstukken II 2010-2011, 32761, nr. 2.
188 WRR rapport *i*Overheid, p. 13.
189 WRR rapport *i*Overheid, p. 17.
190 WRR rapport *i*Overheid, p. 16.

als het ware het kabinet een spiegel voor; ook de overheid zelf dient naar de burger toe transparant te zijn met betrekking tot de verwerking van zijn of haar persoonsgegevens.
In de kabinetsreactie op het WRR-rapport *i*Overheid wordt benadrukt dat de nationale overheid niet in staat is of zal zijn over datastromen in de informatiesamenleving (*i*Samenleving) in den brede regie te voeren, of die naar zich toe te trekken. Bovendien acht het kabinet het wenselijk noch noodzakelijk om te streven naar een regierol in de *i*Samenleving. "De overheid heeft niet tot taak alle risico's te beheersen; zij heeft echter wel tot taak de burger in de *i*Samenleving optimaal te voorzien van mogelijkheden om zelf (mede) sturing te geven aan de *i*Samenleving, bijvoorbeeld met behulp van effectieve correctie- en inzagerechten".[191] Het kabinet ziet veeleer een rol weggelegd voor burgers en stelt vanuit deze stellingname dat het vergroten van mogelijkheden van burgers om hun gegevens te controleren en te laten corrigeren een 'countervailing power' op gang kan brengen. Hieronder verstaat het kabinet een tegenkracht waarvan een preventieve werking richting gegevensbeheerders, -eigenaren en opdrachtgevers bij de overheid zal uitgaan. "Zij worden dan immers meer gedwongen de gegevensverwerking intern goed op orde te hebben".[192] Het kabinet zal daarom onderzoeken op welke wijze de informatiepositie van de burger verder kan worden versterkt door uitbreiding van de functionaliteit van de website 'MijnOverheid'. "Uitgangspunt van de overheidsbrede visie op dienstverlening is dat burgers, bedrijven en instellingen online inzicht hebben in de gegevens die de overheid van hen heeft en de mogelijkheid hebben een verzoek te doen om deze gegevens te laten wijzigen als ze onjuist zijn".[193] Kort geformuleerd, kunnen we vaststellen dat het kabinet een belangrijke rol voor transparantie ziet weggelegd.

2.2.4 Recapitulatie

Op grond van de artikelen 33 en 34 Wbp dient de verantwoordelijke de betrokkene te informeren indien persoonsgegevens van hem of haar worden verwerkt. In het bijzonder dient de verantwoordelijke zijn identiteit bekend te maken alsmede de doeleinden van de verwerkingen waarvoor de gegevens bestemd zijn. Voor het overige kennen de artikelen 33 en 34 open normen. Met betrekking tot regelgeving van cookies is relevant dat de informatieplicht uit de Wbp hierop onverkort van toepassing is. Diverse instanties hebben gewezen op het belang van transparantie in relatie tot de verwerking van persoonsgegevens. Ook het kabinet heeft bij meerdere gelegenheden dit belang benadrukt, maar ziet geen reden om de artikelen 33 en 34 Wbp te herzien. Wel is het kabinet voornemens om de verantwoordelijke te verplichten de vastgestelde bewaartermijnen bekend te maken en te verduidelijken wat er na afloop van die termijn gebeurt met de verwerkte persoonsgegevens. Tevens overweegt het kabinet een afzonderlijke regeling te introduceren met specifieke transparantieverplichtingen bij het toepassen van profileringen,

191 Kamerstukken II 2011-2012, 26643, nr. 211, p. 2.
192 Kamerstukken II 2011-2012, 26 643, nr. 211, p. 9 e.v.
193 Kamerstukken II 2011-2012, 26643, nr. 211, p. 15.

met inbegrip van een explicitering van het doel van de verwerking en de daarbij gehanteerde categoriseringen. Tenslotte laat de kabinetsreactie op het WRR-rapport *i*Overheid zien dat het belang van transparantie als instrument voor een zekere mate van *counterveiling power* van burgers toeneemt.

2.3 De privacyverklaring als instrument ter uitwerking van de informatieplicht

De voorgaande analyse van de artikelen 33 en 34 Wbp laat zien dat de wetgever niet expliciet heeft geregeld dan wel beoogd te regelen op welke wijze (mondeling, schriftelijk of elektronisch) of in welke vorm (bijvoorbeeld per e-mail of SMS) de verplichte informatie aan de betrokkene dient te worden verstrekt. Uit de MvT lijkt te kunnen worden opgemaakt dat dit een bewuste keuze is geweest; er wordt vermeld dat op velerlei wijze de verplichte informatie kan worden verstrekt en de wetgever schetst ter aanvulling enkele voorbeelden.[194] In de praktijk blijken verantwoordelijken veelal een online privacyverklaring te gebruiken ter voldoening van de informatieplicht indien betrokkenen via een website persoonsgegevens verstrekken. Hoewel de verantwoordelijke niet verplicht is om de betrokkene via het instrument van de online privacyverklaring te informeren, is de realiteit dat de verantwoordelijke nagenoeg alleen door middel van een privacyverklaring aan zijn informatieverplichting kan voldoen wanneer de onderlinge communicatie uitsluitend langs elektronische weg plaatsvindt. De betrokkene dient immers vooraf te worden geïnformeerd, dat wil zeggen voordat persoonsgegevens van hem worden verwerkt. Het sturen van bijvoorbeeld een brief of het verzenden van een SMS of e-mail aan de betrokkene lijkt hier niet realistisch aangezien de verantwoordelijke dikwijls niet in het bezit is van de hiervoor benodigde gegevens. De MvT stelt zich op het standpunt dat het voor de verantwoordelijke weinig bezwaarlijk zal zijn om langs dezelfde weg de betrokkene vooraf uitgebreid te informeren over wat er met zijn persoonsgegevens gebeurt als de weg waarlangs de gegevens werden verzameld.[195] De Groep Gegevensbescherming Artikel 29 heeft diverse opinies gepubliceerd over de mogelijke verschijningsvormen en de inhoud van een privacyverklaring.[196] Relevant zijn hier ook de door het Cbp uitgegeven 'Richtsnoeren Publicatie van persoonsgegevens op Internet'[197] en 'Informatieblad informatieplicht'.[198] Daarin merkt de toezichthouder op dat de informatieplicht uit de Wbp kan worden ingevuld door het publiceren van een privacyverklaring op de website. Thijssen is van mening dat de verantwoordelijke het best de betrokkene informeert via de weg waarlangs hij diens

194 Kamerstukken II 1997-1998, 25892, nr. 3, p. 152 e.v.

195 Kamerstukken II 1997-1998, 25892, nr. 3, p. 152.

196 Onder meer Groep gegevensbescherming Artikel 29-2000, Groep gegevensbescherming Artikel 29-2001, Groep gegevensbescherming Artikel 29-2004 en Groep gegevensbescherming Artikel 29-2009(2).

197 Cbp Richtsnoeren Persoonsgegevens op internet, p. 27.

198 Cbp Informatieblad, p. 2.

gegevens verkreeg[199], en acht het in aanvulling daarop voldoende dat de betreffende informatie in een privacystatement op een internetpagina staat.[200] Ook andere auteurs zoals Van Esch en Blok refereren aan het gebruik van een privacyverklaring ter voldoening aan de informatieplicht, en wel door middel van een link op de homepage en op iedere pagina aan de hand waarvan gegevens worden verzameld.[201] Naar de visie van Holleman is een privacystatement een verklaring waarin de aanbieder van de website uiteenzet hoe hij omgaat met persoonsgegevens van bezoekers van de website.[202] Siemerink benoemt in haar onderzoek naar de overeenkomst tussen Internet Service Providers en de consument de privacyverklaring als een praktische oplossing om te verklaren hoe een verwerker, in dit geval een Internet Service Provider, omgaat met de privacy van zijn klanten.[203] Dubbeld heeft het over een specifiek document dat via een website beschikbaar is en waarin uiteen wordt gezet welke privacyregels het bedrijf hanteert.[204] Nouwt bespreekt in zijn onderzoek diverse zelfreguleringsinitiatieven ter bescherming van persoonsgegevens.[205] In dat kader, en in het bijzonder in verband met de bescherming van de persoonsgegevens van kinderen die online worden verzameld, verwijst hij naar de Verenigde Staten. Daar is in de Children's Online Privacy Protection Act wettelijk geregeld dat de aanbieder van een website die is gericht op kinderen verplicht is een privacy policy of privacystatement op de homepage van de website of van de online aangeboden dienst te plaatsen.[206] Jones en Tahri refereren aan artikel 10 en 11 van de Privacyrichtlijn, en stellen dat op grond van deze artikelen de te verstrekken informatie "will typically be provided, principally, through a website privacy statement set out on a page on the site and prominently linked from the site's other pages".[207] Ook waar het meer specifiek over het gebruik van cookies gaat, wordt door het kabinet Rutte gewezen op de mogelijkheid van een privacy statement.[208] Van der Sloot concludeert op basis van de bestaande praktijk dat internetgebruikers doorgaans worden geïnformeerd door middel van een privacy policy die echter veelal slecht te vinden en moeilijk leesbaar is.[209] Versmissen bespreekt de wijze van inbedden van privacy compliance binnen een organisatie, en onderscheidt daarbij 4 onderdelen.[210] Eén zo'n onderdeel betreft het formuleren van het privacybeleid voor die organisatie, waarbij het gaat om zowel intern

199 Thijssen, p. 238.
200 Thijssen, p. 236.
201 Van Esch & Blok, p. 220.
202 Holleman 2003, p. 253. Zo ook Holleman 2005, p. 168.
203 Siemerink, p. 65.
204 Dubbeld, p. 133.
205 Nouwt 2005, p. 76 e.v.
206 Nouwt 2005, p. 85 e.v.
207 Jones & Tahri, p. 618.
208 Kamerstukken II 2010-2011, 32549, nr. 7, p. 28.
209 Van der Sloot 2011-a, p. 1494.
210 Versmissen hanteert de volgende werkdefinitie van privacy compliance: "Het naleven van wet- en regelgeving en andere normen met betrekking tot de omgang met persoonsgegevens". Versmissen, p. 6.

privacybeleid als om richtlijnen toegespitst op specifieke thema's. "Een bijzonder type algemeen privacybeleid vormt een privacyverklaring voor de website(s) van de organisatie."[211] Uit het voorgaande wordt in ieder geval duidelijk dat de privacyverklaring breed wordt geaccepteerd als te hanteren instrument bij de invulling van de informatieplicht. Daarbij wordt ten aanzien van cookies specifiek opgemerkt dat de huidige praktijk van privacyverklaring onvoldoende invulling geeft aan de noodzakelijke transparantie. Daarmee komt ook het volgende aspect in beeld: de kenbaarheid en verschijningsvorm van de verklaring.

2.3.1 De kenbaarheid en de verschijningsvormen van een privacyverklaring

De betrokkene kan veelal kennisnemen van de inhoud van de privacyverklaring door te 'klikken' op een button in de vorm van een hyperlink. In de MvT wordt de hyperlink als mogelijke verschijningsvorm van de privacyverklaring genoemd: "Op het eerste scherm dat na het inloggen verschijnt en waarbij de betrokkene in de gelegenheid wordt gesteld gegevens over zichzelf in te voeren, kan een extra regel op het scherm verwijzen naar bijvoorbeeld via doorklikken beschikbare informatie over de verwerkingen die geschieden met de gegevens".[212] Een vluchtige verkenning op willekeurig gekozen websites leert dat de door de verantwoordelijken gekozen benaming van een dergelijke 'privacy hyperlink' divers is; 'privacy', 'privacy policy', 'privacy statement', 'privacy verklaring' en 'uw privacy' zijn voorbeelden. De actieve informatieplicht van de verantwoordelijke rechtvaardigt de vraag of een privacyverklaring die door middel van een hyperlink toegankelijk is wel een afdoende middel is ter vervulling van die actieve plicht. De Groep Gegevensbescherming Artikel 29 is van mening dat in elke situatie dat persoonsgegevens worden verzameld de betrokkene daarover de essentiële informatie dient te krijgen op een zodanige manier dat een eerlijke en rechtmatige verwerking is gewaarborgd.[213] In een aanbeveling stelt de Groep dat in het algemeen een privacyverklaring die via een hyperlink beschikbaar is niet de voorkeur verdient, en dat de informatie aan de betrokkene rechtstreeks op het scherm dient te worden verstrekt zonder dat de betrokkene zelf actie hoeft te ondernemen om toegang te krijgen tot de informatie. De Groep geeft dienaangaande meer de voorkeur aan het presenteren van de informatie aan de hand van tekstvensters op het moment dat de persoonsgegevens worden verzameld. Het argument dat de Groep hierbij aanvoert, is dat internetgebruikers in de dagelijkse praktijk niet altijd (mogelijk nooit) de moeite nemen het privacybeleid door te nemen wanneer bij het surfen meerdere websites worden bezocht.[214] Het is echter niet ondenkbaar dat de betrokkene een dergelijk venster uiteindelijk als

---

211 Versmissen, p. 8.

212 Kamerstukken II 1997-1998, 25892, nr. 3, p. 152.

213 Groep Gegevensbescherming Artikel 29-2000, p. 52. Vergelijk De Vries die stelt dat wanneer persoonsgegevens worden verkregen via websites, de betrokkene door de verantwoordelijke dient te worden geïnformeerd alvorens de betrokkene op de verzendknop drukt. De Vries 2009, art. 33 Wbp, aant. 2., p. 605.

214 Groep Gegevensbescherming Artikel 29-2000, p. 52.

hinderlijk zal gaan ervaren, en in het vervolg deze ongelezen zal wegklikken. Van Esch en Blok vinden daarom ook dat het rechtstreeks op het scherm moeten plaatsen van de informatie ondoenlijk is.[215]

2.3.2 De inhoud van een privacyverklaring

In het werkdocument 'Privacy op internet' uit 2000 benadrukt de Groep Gegevensbescherming Artikel 29 dat de gegevensstromen op het Internet enorm snel verlopen en dat de traditionele regels over het informeren van de betrokkene over verwerking en doelstelling vaak niet in acht worden genomen. Voorts stelt de Groep dat er websites zijn met een verklaring omtrent het privacybeleid, waarin wordt aangegeven hoe informatie wordt verwerkt, wat ermee wordt beoogd en hoe betrokkenen hun rechten kunnen doen gelden, maar dat dit beleid niet altijd overeenkomt met het daadwerkelijk beleid en dat zelfs als een privacybeleid wordt beschreven dit niet altijd alle benodigde informatie bevat.[216] In vervolg op dit werkdocument kwam de Groep met een aanbeveling over de informatie die minimaal aan de betrokkene dient te worden verstrekt en het moment waarop dit moet gebeuren indien via een website persoonsgegevens worden verzameld.[217] Het Cbp presenteerde later diverse aanvullingen, waaronder het vermelden van de bewaartermijn van de persoonsgegevens en het meldingsnummer (indien van toepassing) waarmee de verwerking is aangemeld bij het Cbp.[218] Daarbij stelt het Cbp dat de inhoud van een privacyverklaring in duidelijke en begrijpelijke taal dient te worden opgesteld.[219] Ook Holleman heeft een overzicht opgesteld met daarin puntsgewijs weergegeven de elementen die naar zijn mening in een privacyverklaring dienen te worden opgenomen.[220] Hij maakt daarbij een onderscheid tussen commerciële en niet-commerciële websites. In het kader van het onderhavige onderzoek beperk ik mij tot de eerstgenoemde categorie. Daarbij wordt allereerst duidelijk dat de door Holleman genoemde punten in essentie nagenoeg gelijk zijn aan die van de Groep Gegevensbescherming Artikel 29. Holleman is echter specifieker waar het persoonsgegevens betreft die in het kader van marketingactiviteiten door de betrokkene worden verstrekt. Ook is hij stringenter ten aanzien van de informatie over de toezeggingen die door een derde zijn gedaan ten aanzien van vertrouwelijkheid en de mate van beveiliging indien deze derde persoonsgegevens krijgt doorgespeeld van de verantwoordelijke.[221] Holleman wijkt af van de Groep Gegevensbescherming Artikel 29 waar

---

215 Van Esch & Blok, p. 220.

216 Groep Gegevensbescherming Artikel 29-2000, p. 52.

217 Groep Gegevensbescherming Artikel 29-2001, p. 5 e.v.

218 Cbp Richtsnoeren Persoonsgegevens op internet, p. 27.

219 Cbp Richtsnoeren Persoonsgegevens op internet, p. 27. Vergelijk Groep Gegevensbescherming Artikel 29-2000, p. 52: "Om echt informatief te zijn moet de beschrijving van het privacybeleid niet te wijdlopig zijn, een heldere structuur hebben en in duidelijke, begrijpelijke termen een correct beeld geven van het beleid."

220 Holleman 2003, p. 255.

221 Voor de volledigheid vermeld ik dat Holleman van mening is dat in de privacyverklaring tevens de informatie dient te worden opgenomen zoals bepaald in artikel 7:46c lid 1 BW. Deze bepaling ziet

het de informatie over verstrekking naar derde landen betreft. De Groep stelt als minimum voorwaarde dat de verantwoordelijke dient te melden dat persoonsgegevens door hem worden doorgegeven naar landen buiten de Europese Unie, en voorts dat alle door de verantwoordelijke te verstrekken informatie dient te worden gegeven in die talen die op de website worden gebruikt.

Op verzoek van de Europese Commissie[222] heeft de Groep Gegevensbescherming Artikel 29 geadviseerd over een meer uniforme interpretatie van artikel 10 van de Privacyrichtlijn. In het advies stelt de Groep dat op grond van de Privacyrichtlijn de navolgende informatie in ieder geval dient te worden opgenomen in privacyverklaringen:[223]

1. Essentiële informatie die moet worden verstrekt in alle gevallen waarin de betrokkene die informatie nog niet heeft, meer bepaald de identiteit van de voor de verwerking verantwoordelijke en de doeleinden van de gegevensverwerking.
2. Verdere informatie die moet worden verstrekt als dit noodzakelijk is om een eerlijke verwerking te waarborgen, gelet op de specifieke omstandigheden waaronder de gegevens worden verzameld.

Om een indruk te krijgen van het totaal aan aspecten waar informatie via een privacyverklaring over verstrekt dient te worden, wordt de door de Groep Gegevensbescherming Artikel 29 opgestelde lijst van minimaal te verstrekken informatie gecombineerd met de aanvullingen van zowel het Cbp als Holleman. Dit leidt tot het navolgende:

Minimaal aan de betrokkene te verstrekken informatie ingeval via een website persoonsgegevens worden verzameld van een individuele gebruiker volgens de Groep Gegevensbescherming Artikel 29, aangevuld met standpunten Cbp en Holleman.	
1	Vermelding van de identiteit, het fysieke en het elektronische adres van de voor de verwerking verantwoordelijke.
2	Duidelijke vermelding van het doel (de doeleinden) van de verwerking waarvoor de voor de verwerking verantwoordelijke gegevens vergaart via een website.
3	Duidelijke vermelding of het verstrekken van bepaalde informatie verplicht of facultatief is. Verplichte informatie is informatie die noodzakelijk is voor het uitvoeren van de verlangde dienst.
4	Vermelding van het recht dat betrokkenen hebben om, afhankelijk van de situatie, toestemming te geven voor of zich te verzetten tegen de verwerking van persoonsgegevens en van de voorwaarden die daarvoor gelden.

op te verstrekken informatie in het kader van koop op afstand. Die informatie laat ik thans buitenbeschouwing daar ik van mening ben dat die gegevens niet in een privacyverklaring behoren te worden vermeld.

222 COM (200) 265 definitief, p. 27 e.v.

223 Groep Gegevensbescherming Artikel 29-2004, p. 8.

5	Vermelding van het recht op toegang tot en rectificatie en verwijdering van gegevens. Er moet ten eerste worden vermeld tot welke persoon of dienst men zich moet wenden om deze rechten uit te oefenen en ten tweede dat deze rechten zowel on line als op het fysieke adres van de voor de verwerking verantwoordelijke kunnen worden uitgeoefend.
6	Een lijst van ontvangers of categorieën ontvangers waarvoor de verzamelde informatie bestemd is.
7	Bij het vergaren van gegevens dienen websites te vermelden of het verzamelde materiaal aan derden zal worden verstrekt of ter beschikking gesteld, met name bijvoorbeeld aan zakelijke partners of dochterondernemingen, en waarom. De website dient te vermelden dat de derden aan wie de persoonsgegevens door de verantwoordelijke worden verstrekt, de vertrouwelijkheid en de beveiliging van de persoonsgegevens hebben toegezegd (**aanvulling Holleman**).
8	Duidelijke vermelding van het gebruik van automatische procedures voor gegevensvergaring (cookies) alvorens deze voor enigerlei gegevensvergaring worden toegepast. Bij toepassing van dergelijke procedures dient men de betrokkene niet alleen de in deze tabel vermelde informatie te verstrekken, maar hem tevens te informeren over de domeinnaam van de server die de automatische procedures voor gegevensvergaring overbrengt, over het doel en de geldigheidsduur ervan, en over de vraag of instemming ermee noodzakelijk is voor het bezoeken van de site. Verder moet duidelijk worden gemaakt dat elke internetgebruiker de mogelijkheid heeft zich te verzetten tegen het gebruik van de procedures en tevens welke gevolgen het heeft als hij de procedures buiten werking stelt. In het geval dat ook andere voor de verwerking verantwoordelijken bij het vergaren van de persoonsgegevens zijn betrokken, dient men de betrokkene informatie te verschaffen over hun identiteit en over de doeleinden van de verwerking uit het oogpunt van elke voor de verwerking verantwoordelijke.
9	Vermelding van de bewaartermijn van de persoonsgegevens (**aanvulling door Cbp**).
10	Een schets van de beveiligingsmaatregelen die bij de website worden toegepast om de authenticiteit van de site en de integriteit en vertrouwelijkheid van de via het netwerk overgedragen informatie te waarborgen.
11	Indien van toepassing, het meldingsnummer waarmee de verwerking is aangemeld bij het Cbp (**aanvulling door Cbp**).
12	Als is te voorzien dat de voor de verwerking verantwoordelijke de gegevens naar landen buiten de Europese Unie gaat doorgeven, vermelding of in die landen een passende bescherming van de privacy van personen op het punt van de verwerking van persoonsgegevens wordt geboden. In dat geval moet specifieke informatie worden verstrekt over de identiteit en het adres van de ontvangers (fysiek en/of elektronisch adres).
13	Vermelding van naam en adres (fysiek en elektronisch adres) van de dienst of persoon die verantwoordelijk is voor het beantwoorden van vragen betreffende de bescherming

	van persoonsgegevens.
14	De informatie dient te worden verstrekt in alle op de site gebruikte talen en in het bijzonder op die plaatsen waar persoonsgegevens worden verzameld.

Tabel 2.5

De Groep Gegevensbescherming Artikel 29 meent bovendien dat de kennisgeving niet in één enkel document vervat hoeft te zijn, en het denkbaar is dat informatie aan de betrokkene wordt verstrekt in (maximaal) drie stappen (ook wel aangeduid als 'lagen') zolang het totaal voldoet aan de wettelijke eisen.[224] Daarbij is de Groep van mening dat ten gevolge van getrapte kennisgevingen de informatieverstrekking en absorptie door de betrokkene aan kwaliteit wint indien de betrokkene in iedere trap net genoeg gerichte informatie wordt geboden om zich een mening te kunnen vormen en beslissingen te kunnen nemen. "Wanneer de ruimte of tijd voor een mededeling beperkt is, kan een getrapte opmaak de leesbaarheid van de kennisgevingen verbeteren", aldus de Groep.[225] Daarbij maakt men onderscheid in de korte kennisgeving, de beknopte kennisgeving en de volledige kennisgeving. Voor de, volgens de Groep, gewenste inhoud van iedere afzonderlijke trap wordt verwezen naar onderstaande tabellen.

Trap 1 – De korte kennisgeving
Deze Trap moet de betrokkene de wezenlijke informatie bieden die op grond van artikel 33 Wbp vereist is, met name de identiteit van de voor de verwerking verantwoordelijke en de doeleinden van de verwerking - tenzij de betrokkenen daarvan reeds op de hoogte zijn - en alle aanvullende informatie die, gelet op de specifieke omstandigheden, van tevoren moet worden verstrekt om een eerlijke verwerking te waarborgen. Daarnaast moeten duidelijke aanwijzingen worden gegeven over hoe de betrokkene toegang kan krijgen tot aanvullende informatie.

Tabel 2.6

Trap 2 – De beknopte kennisgeving
Middels Trap 2 moet de betrokkene steeds toegang kunnen krijgen tot een kennisgeving die alle op grond van de Wbp vereiste relevante informatie bevat. Die omvat, naargelang de omstandigheden van het geval: • De naam van het bedrijf of organisatie; • Het doel van de gegevensverwerking;

[224] Het advies van de Groep Gegevensbescherming Artikel inzake de getrapte informatieverstrekking geldt zowel voor online als off-line omgevingen. Groep Gegevensbescherming Artikel 29-2004, p. 8.

[225] Groep Gegevensbescherming Artikel 29-2004, p. 8.

• De ontvangers of categorieën ontvangers van de gegevens; • Of het antwoord op de vragen verplicht of vrijwillig is, en tevens de mogelijke gevolgen van het niet-antwoorden; [226] • De mogelijkheid van doorgifte aan derden; • Het recht van toegang, rectificatie en verzet; • Keuzes die de betrokkene heeft. Daarnaast moet een contactpunt worden geboden voor vragen en informatie over verhaalmogelijkheden binnen het bedrijf of organisatie zelf dan wel de gegevens van de dichtstbijzijnde autoriteit voor gegevensbescherming. De beknopte kennisgeving moet zowel on line als na schriftelijk of telefonisch verzoek op papier beschikbaar worden gesteld. De voor de verwerking verantwoordelijken worden aangemoedigd om deze kennisgeving aan te bieden in een tabelformaat om vergelijkingen te vergemakkelijken.

Tabel 2.7

Trap 3 – De volledige kennisgeving
In deze trap dient een volledige privacyverklaring te zijn opgenomen. De inhoud van de privacyverklaring dient te voldoen aan de minimum eisen zoals geformuleerd door de Groep Gegevensbescherming Artikel 29.[227]

Tabel 2.8

Het idee dat de informatieverstrekking – en daarmee ook de privacyverklaring - in meerdere stappen invulling kan krijgen wordt omarmd door het Center for Information Policy Leadership. “Research on how people learn has shown that for notices to be easy to read and understand, they must be short, use plain language, and be presented in a common format. Complete notices tend to be longer and more complex, so it is impossible to have both sets of requirements in one document. A multilayered notice is made up of a condensed notice that contains all the key factors in a way that is easy to understand and is actionable, and a complete notice with all the legal requirements”.[228] Ter ondersteuning bij het opstellen van een privacyverklaring die uit meerdere lagen bestaat, heeft The Center for Information Policy Leadership een stappenplan ontwikkeld.[229] Vermeld kan verder worden dat in het Verenigd Koninkrijk het gebruik van gelaagde privacyverklaringen wordt aangemoedigd door de Information Commissioner’s Office: “Many individuals will be more

226 Met ‘vragen’ wordt in dit kader bedoeld de vragen die op een website worden gepresenteerd ter verkrijging van persoonsgegevens.

227 Groep Gegevensbescherming Artikel 29-2001.

228 The Center for Information Policy Leadership 2007, p. 1. “The Centre for Information Policy Leadership develops initiatives that encourage responsible information governance in today's digital society. Through collaboration with industry leaders, consumer organizations and government representatives, the Centre provides leadership in developing policy to help ensure privacy and information security while balancing economic and societal needs and interests in today’s global information age”. Http://www.informationpolicycentre.com.

229 The Center for Information Policy Leadership 2007.

concerned with receiving the goods, services or benefits that they have applied for. They are unlikely to read a detailed privacy notice, or to make a complaint about the way you handle their personal information, unless they feel their personal information has been handled badly. This is why a 'layered notice' can be useful. This allows you to provide the basic privacy information there and then, but to make more detailed information available elsewhere for those that want it".[230] Ook in Australië hanteert 'the Office of the Privacy Commissioner' een gelaagde privacyverklaring en worden andere (overheids)organisaties gestimuleerd om dit model te gebruiken.[231]

Van Esch en Blok kwalificeren de wijze waarop de Groep Gegevensbescherming Artikel 29 de informatieplicht heeft uitgewerkt als zeer breed.[232] Zij vragen zich af of de verantwoordelijke daadwerkelijk wettelijk verplicht is om alle informatie die de Groep noemt te verstrekken. Voorts menen zij dat, gezien het relatief onschuldige karakter van vele gegevensverwerkingen in het kader van elektronische handel, kan worden aangenomen dat het in het algemeen zal volstaan om de betrokkene te informeren over de identiteit van de verantwoordelijke, de doeleinden van de gegevensverwerking en het gebruik van cookies.[233] De opinie van de Groep Gegevensbescherming Artikel 29 kan worden gezien als een aanbeveling die als doel heeft een bijdrage te leveren aan een doeltreffende en consistente toepassing van de nationale bepalingen.[234] Niet duidelijk is of de aanbevelingen van de Groep Gegevensbescherming Artikel 29 verder reiken dan de titel doet vermoeden.[235] In de literatuur wordt veel discussie gevoerd over dit soort soft law instrumenten, in het bijzonder over de legitimiteit daarvan.[236] Soft law kan worden gedefinieerd als gedragsregels die worden vastgelegd in instrumenten die als zodanig geen verbindende kracht zijn toegekend, maar die desalniettemin in de dagelijkse praktijk (van gegevensverwerking) bepaalde (indirecte) juridische effecten kunnen bewerkstelligen.[237] Voorbeelden van soft law instrumenten zijn aanbevelingen, (gedrags)codes, adviezen, conclusies en richtsnoeren.[238] Hiervoor is gerefereerd aan de Richtsnoeren die het Cbp heeft opgesteld ter invulling van de open normen uit de Wbp, en die voor de verantwoordelijke handvatten moeten bieden in geval deze persoonsgegevens verwerkt die

230 Privacy notices code of practice, p. 11.

231 Australian Government. In de privacyverklaring wordt verwezen naar het advies van de Groep Gegevensbescherming Artikel 29 inzake de gelaagde privacyverklaringen: "This Layered Notices format... and endorsed in Opinion WP 100 by the Article 29 Committee of European Data Protection Commissioners."

232 Van Esch & Blok, p. 119.

233 Van Esch & Blok, p. 220.

234 Groep Gegevensbescherming Artikel 29-2001, p. 2 e.v.

235 Zie Moerel, p. 292.

236 Zie Luijendijk & Senden.

237 Luijendijk & Senden, p. 3.

238 Senden, p. 507. Zie in dit kader ook Bigo et al., p. 117 e.v. en Barkhuysen & Van Emmerik.

zijn verkregen via zijn website.[239] Over deze Richtsnoeren merkt het Cbp het volgende op in het Jaarverslag 2008: “De CBP *Richtsnoeren Publicatie van persoonsgegevens op internet* vormen de norm. Voor verantwoordelijken bevatten de richtsnoeren een gedetailleerde uitwerking van alle voor hen relevante artikelen uit de Wbp. Voor betrokkenen zijn met name het recht op correctie of verwijdering en het recht op intrekken van toestemming van belang”.[240] Over de privacyverklaring wordt in de Richtsnoeren opgemerkt dat een goede uitvoering van de informatieplicht gestalte kan krijgen via het publiceren van een privacyverklaring, waarbij de verklaring in duidelijke en begrijpelijke taal moet zijn opgesteld, goed vindbaar moet zijn en bij voorkeur op te roepen vanuit elk onderdeel van de website. Tevens wordt in de Richtsnoeren geëxpliciteerd dat een privacyverklaring bij een publicatie op het Internet minimaal de elementen moet bevatten zoals aanbevolen door de Groep Gegevensbescherming Artikel 29.[241] Hoewel het Cbp stelt dat de Richtsnoeren de norm vormen, is de juridische status en de bindende kracht van dit soft law instrument, zoals hiervoor al kort besproken, niet duidelijk. Groenhuijsen constateert dat onder het begrip ‘uitvoeringsmaatregelen’ diverse varianten vallen als beleidsregels, beleidsnotities, pseudobeleidsregels, richtlijnen, handleidingen, brochures en toelichtingen.[242] Hij tekent vervolgens aan dat het van sommige publicaties onvoldoende duidelijk is of ze een voorlichtend karakter hebben dan wel dat het verkapte beleidsregels zijn.[243] “De functie van de verschillende vormen van ‘uitvoeringsregelingen’ is bovendien niet steeds identiek. Het uitgangspunt lijkt te zijn dat ze zijn bedoeld om duidelijkheid te beiden inzake de nadere uitwerking van de wettelijke bepalingen. Het achterliggende belang lijkt dan rechtszekerheid te zijn”.[244] Volgens Groenhuijsen zou uit nadere studie naar uitvoeringsregelingen kunnen blijken dat sommige uitvoeringsmaatregelen vooral op verduidelijking en op rechtszekerheid gericht zijn, terwijl andere uitvoeringsmaatregelen primair de rechtsontwikkeling en de inhoudelijke kwaliteitsverbetering van in wetgeving neergelegde regelgeving zouden kunnen dienen.[245] Essers stelt dat beleidsregels onder bepaalde voorwaarden door de Hoge Raad als recht in de zin van artikel 79 RO worden aangemerkt. Daartoe dienen deze regels aan de volgende voorwaarden te voldoen:[246]

1. het moet gaan om door een bestuursorgaan binnen zijn bestuursbevoegdheid vastgestelde regels over de uitoefening van zijn beleid;
2. deze beleidsregels moeten behoorlijk bekend zijn gemaakt;

---

239 Cbp Richtsnoeren Persoonsgegevens op internet.
240 Cbp Jaarverslag 2008, p. 17.
241 Cbp Richtsnoeren Persoonsgegevens op internet, p. 27.
242 Groenhuijsen, p. 201.
243 Groenhuijsen, p. 204. Groenhuijsen doelt in dezen met name op het fiscale recht.
244 Groenhuijsen, p. 202.
245 Groenhuijsen, p. 205.
246 HR 28 maart 1990, BNB 1990/194 (*Leidraadarrest*).

3. de beleidsregels moeten zich er naar inhoud en strekking toe lenen tegenover de bij de desbetreffende regeling betrokkenen als rechtsregel te worden toegepast.

"In de regel zullen leidraden, goedkeurende en interpretatieve besluiten alsmede standaardvoorwaarden aan deze door de Hoge Raad gestelde voorwaarden voldoen", aldus Essers.[247] Desgevraagd antwoordt het Cbp dat de Richtsnoeren dienen te worden opgevat als een verduidelijking van de wijze waarop de open normen dienen te worden ingevuld, het geen beleidsregel betreft, en de Richtsnoeren niet kunnen worden aangemerkt als recht in de zin van artikel 79 RO.[248]

2.3.3 Verplichtstellen van het gebruik van een privacyverklaring door een belangenorganisatie

Een belangrijke vraag bij de status van de privacyverklaring houdt verband met de sturing van belangenorganisaties. In hoeverre beogen en kunnen brancheorganisaties hun leden houden aan het hanteren en op een bepaalde wijze uitwerken van een privacyverklaring? Illustratief is hier de werkwijze van de belangenorganisatie Thuiswinkel.org. Deze organisatie is opgericht op 20 december 2000 en behartigt de belangen van verkopers op afstand.[249] De leden van Thuiswinkel.org hebben de verplichting opgelegd gekregen een privacyverklaring op hun website te plaatsen. Het naleven van deze verplichting is een voorwaarde voor het verkrijgen van het lidmaatschap van de belangenorganisatie. Voorts dient de verantwoordelijke die lid is van Thuiswinkel.org de inhoud van de privacyverklaring te laten beoordelen, en eventueel in overleg te laten aanpassen, door een extern juridisch adviesbureau.

> Lidmaatschap Thuiswinkel.org en het Thuiswinkel Waarborg Versie d.d. 16-02-2009
>
> 4. Voor het aanvragen van het gewone lidmaatschap dient de aanvrager gebruik te maken van het daartoe door Thuiswinkel.org beschikbaar gestelde formulier. Bij de aanvraag dienen een recent uittreksel van de inschrijving bij de Kamer van Koophandel, een financieel jaarverslag en de teksten van de door het bedrijf gehanteerde algemene voorwaarden en het privacy statement overlegd te worden.
>
> 6. Het privacy statement en de algemene voorwaarden worden ter beoordeling voorgelegd aan een extern juridisch adviesbureau dat de teksten toetst aan de hand van de wettelijke regels en de gedragsregels van de Thuiswinkel.org. Indien aanpassing noodzakelijk is, stemt het juridisch adviesbureau dit rechtstreeks met de aanvrager af. Het juridisch adviesbureau brengt aan de hand van haar bevindingen een advies uit.

Verplichtingen voor de verantwoordelijke tot het gebruik van een privacyverklaring kunnen tevens worden vastgelegd in een door een branche opgestelde gedragscode zoals bedoeld

247 Essers, p. 15.

248 Telefonisch overleg tussen het Cbp en Verhelst, de dato 5 oktober 2011.

249 Zie ook de website www.thuiswinkel.org.

in artikel 25 Wbp. Het betreft hier een vorm van zelfregulering op basis waarvan de algemene normen van de Wbp per sector kunnen worden geconcretiseerd.[250] Organisaties die een gedragscode willen vaststellen kunnen conform artikel 25 lid 1 Wbp het Cbp verzoeken te verklaren dat de daarin opgenomen regels een juiste uitwerking vormen van wetgeving over de verwerking van persoonsgegevens.[251] Een door het Cbp verstrekte verklaring van goedkeuring is op grond van artikel 25 lid 5 Wbp geldig voor de duur van maximaal vijf jaar, te berekenen vanaf het tijdstip waarop de verklaring bekend is gemaakt.[252] Zoals volgt uit onderstaand overzicht zijn er zes gedragscodes waaraan het Cbp een verklaring van goedkeuring heeft verstrekt en die niet verlopen zijn.[253]

Gedragscode(s) waaraan het Cbp een verklaring van goedkeuring heeft verstrekt en waarvan de termijn niet is verstreken	**Jaar van goedkeuring**
Privacygedragscode sector particuliere onderzoeksbureaus van de Vereniging van Particuliere Beveiligingsorganisaties	2009
Gedragscode van de Nederlandse Vereniging van de Research-georiënteerde Farmaceutische Industrie (Nefarma).	2010
Gedragscode Verwerking Persoonsgegevens Financiële Instellingen	2010
Gedragscode Verwerking Persoonsgegevens van de Nederlandse Vereniging van (Handels)informatiebureaus	2011
Gedragscode voor Onderzoek & Statistiek	2011
Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars	2012

Tabel 2.9

De Gedragscode Verwerking Persoonsgegevens Financiële Instellingen is van toepassing op Financiële instellingen die (i) lid zijn van de Nederlandse Vereniging van Banken, (ii) aangesloten zijn bij Rabobank Nederland of (iii) lid zijn van het Verbond van Verzekeraars.[254] In vergelijking met de overige hiervoor genoemde gedragscodes is deze gedragscode de enige die de verantwoordelijke de verplichting oplegt om op de website een privacyverklaring op te nemen met daarin informatie over het beleid met betrekking tot via het Internet verkregen persoonsgegevens.

> Artikel 4.10 Gedragscode Verwerking Persoonsgegevens Financiële Instellingen
> Een Financiële instelling kan in het kader van de bedrijfsvoering via het internet Persoonsgegevens van een Betrokkene, die een Financiële instelling via dit medium

250 Kamerstukken II 1997-1998, 25892, nr. 3, p. 128.
251 Cbp Brochure Gedragscodes, p. 7.
252 Bekendmaking vindt plaats door middel van publicatie in de Staatscourant.
253 Peildatum 18 januari 2012. Voor een actueel overzicht wordt verwezen naar de website van het College bescherming persoonsgegevens: www.cbpweb.nl.
254 Artikel 3.1.1 Gedragscode Verwerking Persoonsgegevens Financiële Instellingen.

benadert, vastleggen en verder verwerken. Financiële instellingen zullen via een privacy statement op de betreffende website informatie beschikbaar stellen over het beleid met betrekking tot de door middel van het internet verkregen Persoonsgegevens. Het privacy statement bevat minimaal de informatie als bedoeld in artikel 4.7 Gedragscode.

Uit artikel 4.7 en 4.9 van deze gedragscode valt op te maken dat waar het de inhoud van de privacyverklaring betreft in de bewoording aansluiting wordt gezocht bij artikel 33 lid 2 en 3 Wbp. Immers, de verantwoordelijke dient op grond van artikel 4.7 Gedragscode de betrokkene te informeren over zijn identiteit en de doeleinden van de verwerking. Voorts dient hij op grond van artikel 4.9 Gedragscode nadere informatie te verstrekken indien dat, gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is uit oogpunt van het waarborgen van een behoorlijke en zorgvuldige verwerking.

> Artikel 4.7 Gedragscode Verwerking Persoonsgegevens Financiële Instellingen
> Indien Persoonsgegevens worden verzameld bij de Betrokkene, informeert de Verantwoordelijke de Betrokkene over zijn identiteit en de doeleinden van de Verwerking van persoonsgegevens van de Betrokkene, tenzij de Verantwoordelijke op goede gronden mag aannemen dat de Betrokkene daarvan reeds op de hoogte is. Aan deze informatieplicht wordt voldaan vóór het moment van verkrijging.

> Artikel 4.9 Gedragscode Verwerking Persoonsgegevens Financiële Instellingen
> Indien het, gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is uit oogpunt van het waarborgen van een behoorlijke en zorgvuldige Verwerking van Persoonsgegevens, zal in aanvulling op de informatie als aangegeven in 4.7 en 4.8 Gedragscode nadere informatie worden verstrekt aan de Betrokkene.

Vastgesteld kan worden dat bij de in de privacyverklaring op te nemen inhoud geen aansluiting wordt gezocht bij de nadere concretisering conform de Cbp-Richtsnoeren.[255] Dat terwijl het Cbp heeft aangegeven hierbij de standaard te hebben gezet.[256] De in de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen opgenomen verplichting om een privacyverklaring op de website te doen opnemen lijkt daarom op het eerste oog nauwelijks een meerwaarde te hebben, aangezien qua op te nemen inhoud wordt teruggevallen op de normen uit artikel 33 lid 2 en 3 Wbp en artikel 34 lid 2 en 3 Wbp. Een voordeel is mogelijk wel gelegen in de verplichting dát er een privacyverklaring op de website moet worden opgenomen. Het is daarom interessant te bezien of, en in hoeverre,

255 Cbp Richtsnoeren Persoonsgegevens op internet.
256 Cbp Jaarverslag 2008, p. 17.

een dergelijke verplichting een effect heeft op de naleving van de informatieplicht. In het empirisch onderzoek (hoofdstuk 4) zal daar nader aandacht aan worden geschonken.

2.4 Handhaving van de informatieplicht

Het Cbp ziet onder meer toe op de naleving en de handhaving van de Wbp.[257] De wetgever heeft door het instellen van het Cbp uitvoering gegeven aan artikel 28 van de Privacyrichtlijn, waarin het bestaan van een toezichthoudende autoriteit uitdrukkelijk is voorzien, en waarin voorts is bepaald dat deze autoriteit zijn taak in volledige onafhankelijkheid dient te vervullen. Het voorgaande betekent dat het Cbp toezicht moet houden op verantwoordelijken en meer concreet of zij de informatieplicht wel nakomen. Ook zal ze tot handhaving hebben over te gaan indien de informatieplicht niet of niet volledig wordt nagekomen. Zo kan het Cbp op grond van artikel 66 Wbp een bestuurlijke boete opleggen indien de verantwoordelijke niet voldoet aan zijn informatieplicht. Alsook heeft het Cbp de mogelijkheid om bestuursdwang toe te passen of een last onder dwangsom op te leggen.[258]

Het is niet ondenkbaar dat de verantwoordelijke niet of niet volledig aan zijn informatieplicht voldoet. In paragraaf 2.2.3 is het onderzoek van Zwenne et al. besproken waaruit volgt dat (i) de open normen in relatie tot de informatieplicht tot interpretatiemoeilijkheden leiden, (ii) de informatieplicht bij weinig verantwoordelijken bekend is en (iii) de informatieplicht door de verantwoordelijke te generiek wordt ingevuld.[259] In een brief uit 2004 aan de minister van Justitie onderschrijft het Cbp dat de artikelen 33 en 34 Wbp veel open normen bevatten die rechtsonzekerheid met zich meebrengen. Het College stelt dat deze onzekerheid onnodige nalevingkosten veroorzaakt. Ook kondigt het Cbp aan de informatieplicht als een hoofdthema te agenderen voor 2005. Tenslotte maakt het Cbp kenbaar dat het zal werken aan een standaardisering van de informatieplicht, door het nader invullen van de huidige open normen dan wel door aanpassing van de Wbp.[260] In 2005 benadrukte de voorzitter van het Cbp, Kohnstamm, dat het College erop zal toezien dat verantwoordelijken beter, sneller en effectiever aan de informatieplichten voldoen, waarbij hij als instrumenten ook handhaving en zelfregulering noemt.[261]

---

257 Het Cbp ziet tevens toe op de naleving en handhaving van de Wet Gemeentelijke Basisadministratie en de Wet Politieregisters.

258 Voor een uitgebreid overzicht over de verantwoordelijkheden van het Cbp zie onder meer Bitter en De Hert 2009.

259 Zwenne et al., p. 170 e.v.

260 Cbp Brief aan Minister van Justitie 2004 onder Voorstel 10.

261 Holvast, p. 116.

Is het realistisch te veronderstellen dat het Cbp ambtshalve of op verzoek van een betrokkene tot actie over zal gaan indien een verantwoordelijke geen privacyverklaring op zijn website heeft dan wel de privacyverklaring in inhoudelijke zin onvoldoende invulling geeft aan de informatieplicht? Cuijpers schat die kans niet hoog in.[262] Zij verwijst onder meer naar de jaarverslagen van het Cbp waarin wordt vermeld dat men zich primair richt op problemen die zijn gerezen in bepaalde sectoren of met betrekking tot bepaalde vormen van gegevensverwerking. Cuijpers is van mening dat er maar zelden door het Cbp onderzoek wordt gedaan naar een specifieke verantwoordelijke die ervan beticht wordt het recht op informationele privacy te schenden en dat het initiatief voor rechtsbescherming veelal bij de betrokkenen zelf blijft rusten.[263] Bitter constateert dat het Cbp in lang niet alle gevallen, zelfs wanneer er sprake is van een bredere problematiek dat het concrete probleem van een enkel individu overstijgt, zal kunnen optreden. Hij wijst daarbij op de prioriteitsstelling die in de MvT wordt aangehaald en die in de rechtspraak wordt bevestigd.[264] Naar de mening van Dommering is belangenbehartiging ten behoeve van individuele burgers door het Cbp een illusie. “Door de omvang en complexiteit van het gegevensverkeer en –opslag kunnen zij zich daar niet meer mee bezighouden. Zij hebben zich teruggetrokken op hun kerntaken, waarin nog slechts plaats is voor selectief vervolgingsbeleid als daarbij een voldoende algemeen belang is betrokken”.[265] In het jaarverslag 2007 stelt het Cbp met betrekking tot de toezichthoudende taak dat tot 2007 een vier sporen beleid is bewandeld, te weten: het bevorderen van bewustwording en van normontwikkeling, het op de voet volgen van technologische ontwikkelingen en het in voorkomende gevallen handhavend optreden. Dit beleid heeft het Cbp in 2007 losgelaten. De prioriteit werd verlegd naar het doen van onderzoek en het handhavend optreden, zodat bewustwording van de normen en naleving van de wet beter en krachtiger kon worden gestimuleerd en afgedwongen. “Deze wijziging heeft tot gevolg dat in geval van verzoeken om hulp en bijstand, de prioriteit zal liggen bij ernstige overtredingen met een structureel karakter en die grote gevolgen heeft voor een flink aantal burgers of voor groepen van burgers”, aldus het Cbp.[266]

Het kabinet Balkenende IV ziet drie taken weggelegd voor het Cbp: een adviserings-, wetgevings- en toezichthoudende taak. Ten aanzien van de adviseringstaak stelt het kabinet dat het Cbp hierop minder nadruk zal gaan leggen. De redenen hiervoor zijn tweeledig. Ten eerste leidt naar de mening van het kabinet al te intensieve advisering tot potentiële conflicten met de handhavende rol, en ten tweede zijn de middelen van het Cbp te

262 Cuijpers, p. 217. Voor de volledigheid dient te worden vermeld dat Cuijpers haar mening poneert in 2004.
263 Cuijpers, p. 217.
264 Bitter, p. 63.
265 Dommering 2010, p. 88.
266 Cbp Jaarverslag 2007, p. 3 e.v. Zie in dit kader Koops, p. 169.

beperkt.[267] Het kabinet wil niet tornen aan de rol van het Cbp als adviseur op het gebied van wetgeving. Het beargumenteert dit voornemen door te stellen dat deze rol van het Cbp geen vrijblijvende kwestie is, maar voortvloeit uit de Privacyrichtlijn.[268] Met betrekking tot de toezichthoudende rol van het Cbp tekent het kabinet Balkenende IV vooraleerst aan dat uit de evaluatierapporten over de Wbp de conclusie kan worden getrokken dat er over de hele linie sprake is van een nalevingstekort ten aanzien van deze wet. Derhalve stelt het kabinet dat daaraan iets kan worden gedaan door de handhavingsmogelijkheden van het Cbp te versterken.[269]
In reactie op het kabinetsstandpunt wijst het Cbp vooraleerst op de constatering van het kabinet dat het Cbp adequate boete- en handhavingsbevoegdheden nodig heeft om een robuuste toezichthouder te zijn, en stelt dat onafhankelijkheid en de rolvastheid van de toezichthouder hierbij essentieel zijn. Voorts expliciteert het Cbp dat de focus zal liggen op handhaving van de wet, en dat dit betekent dat het de bevoegdheden met name zal inzetten op die zaken waar sprake is van structurele overtreding van de Wbp die grote groepen mensen raakt en waar het Cbp met zijn bevoegdheden kan optreden.

In het licht van het voorgaande is de kans klein dat het Cbp in beweging zal komen indien de betrokkene zich wendt tot het Cbp met de klacht dat de verantwoordelijke geen privacyverklaring op zijn website heeft of dat de privacyverklaring die de verantwoordelijke op zijn website heeft doen plaatsen onvoldoende van inhoud is om voldaan te hebben aan de informatieplicht. Het Cbp zal in dit geval immers een afweging maken tussen het individuele belang van de betrokkene en de bredere belangen die het Cbp wil behartigen vanuit zijn prioriteitsstelling. Daarbij zal het Cbp mede overwegen wat de schade (vermogensschade of ander nadeel) is die de betrokkene mogelijk heeft geleden of lijdt vanwege het niet of niet geheel nakomen van de informatieplicht door de verantwoordelijke. Deze schade zal juist waar het de informatieplicht aangaat veelal beperkt zijn, met als waarschijnlijk gevolg dat het Cbp niet tot handhaving over zal gaan.

2.5 Rechtsmiddelen van de betrokkene

De betrokkene kan besluiten om de naleving van de informatieplicht bij de rechter af te dwingen conform artikel 50 lid 1 Wbp. Tevens kan de betrokkene op grond van artikel 49 Wbp een schadeprocedure starten; de betreffende bepaling geeft de betrokkene een

267 Kamerstukken II 2009–2010, 31051, nr. 5, p. 25. Zie in dit kader Duthler, p. 60.
268 Kamerstukken II 2009–2010, 31051, nr. 5, p. 26. Zie ook Handelingen I 2010-2011, nr. 27, item 11, p. 52.
269 Kamerstukken II 2009–2010, 31051, nr. 5, p. 26.

zelfstandige handhavingsgrond ter verkrijging van schadevergoeding. Dit artikel is dwingendrechtelijk van aard en afwijkende bepalingen in overeenkomsten zijn nietig.[270]

Op grond van artikel 49 lid 3 Wbp is de verantwoordelijke jegens de betrokkene aansprakelijk voor de schade die of het nadeel dat de betrokkene lijdt en voortvloeit uit het door de verantwoordelijke niet-nakomen van de bij of krachtens de Wbp gegeven voorschriften. Het is aannemelijk dat met 'schade' zoals genoemd in artikel 49 lid 3 Wbp wordt bedoeld vermogensschade, daar artikel 49 lid 2 Wbp zich richt op schadevergoeding op grond van een 'nadeel dat niet gelegen is in vermogensschade', ook wel immateriële schade genoemd. Hiermee wordt gedoeld op ongenoegens zoals lichamelijke pijn, geestelijk leed of aantasting van de persoon van de benadeelde.[271] Het bepalen van de hoogte van de vergoeding in verband met de door de betrokkene geleden immateriële schade is geen eenvoudige opgave. Het EHRM stelt in dit verband dat de toe te wijzen vergoeding proportioneel en voldoende moet zijn.[272]
Van belang is tevens artikel 49 lid 1 Wbp dat bepaalt dat iemand die schade lijdt, doordat ten opzichte van hem in strijd wordt gehandeld met de bij of krachtens de Wbp gegeven voorschriften, onverminderd een beroep kan doen op andere wettelijke regels. Deze 'andere wettelijke regels' kunnen bijvoorbeeld worden gezocht in de onrechtmatige daad, zoals bepaald in artikel 6:162 BW. Dit volgt ook uit de MvT waarin wordt aangetekend dat overtredingen van de informatieplicht zullen leiden tot onrechtmatige verwerkingen.[273]

2.6 Samenvatting en conclusies

Op grond van de artikelen 33 en 34 Wbp dient de verantwoordelijke de betrokkene te informeren indien er persoonsgegevens van hem of haar worden verwerkt. Deze bepalingen zijn in de Wbp opgenomen ter implementatie van de artikelen 10 en 11 uit de Privacyrichtlijn. Ook de artikelen 35 en 41 lid 1 Wbp kennen een informatieplicht die de verantwoordelijke in voorkomende gevallen in acht dient te nemen. Op grond van de artikelen 33 en 34 Wbp dient de verantwoordelijke zijn identiteit bekend te maken alsmede de doeleinden van de verwerkingen waarvoor de gegevens bestemd zijn. Voor het overige moet de verantwoordelijke die informatie aan de betrokkene verstrekken, die nodig is gelet op de aard van de gegevens en/of de omstandigheden waaronder de gegevens worden

270 Kamerstukken II 1997-1998, 25892, nr. 3, p. 176.

271 Zie in dit kader EHRM, 17 juli 2008 (*I v. Finland*), nr. 20511/03, paragrafen 47 en 53, alwaar een vergoeding ter compensatie van geleden niet-geldelijke schade wordt toegekend. Voor een uitgebreide bespreking van dit arrest zie De Hert 2011, p. 47 e.v.

272 EHRM, 25 november 2008 (*Armoniene v. Lithuania*), nr. 36919/02, paragrafen 45 en 52. Vergelijk De Hert die op basis van dit arrest concludeert dat de vergoeding redelijk doch substantieel moet zijn. De Hert 2011, p. 51 e.v.

273 Kamerstukken II 1997-1998, 25892, nr. 3, p. 149.

verkregen en/of het gebruik dat van de gegevens wordt gemaakt. Hiernaast is nog de nadere regelgeving voor cookies relevant. De regelgeving met betrekking tot het toepassen en uitlezen van cookies is vastgelegd in het Besluit universele dienstverlening en eindgebruikersbelangen, maar zal op termijn worden geïmplementeerd in de Telecommunicatiewet. Naar verwachting zal de Wbp in aanvulling onverkort van toepassing worden verklaard. Dit heeft tot gevolg dat de verantwoordelijke bij het gebruik van cookies behalve de specifieke regeling in de Telecommunicatiewet ook de artikelen 33 en 34 Wbp in acht moet nemen.

Uit de evaluatie van de Wbp uitgevoerd door Zwenne et al. kwam naar voren dat de informatieplicht niet of nauwelijks bekend is bij verantwoordelijken. Dit beeld lijkt enigszins te worden afgezwakt in het empirische vervolgonderzoek. Ook blijkt uit de studie van Zwenne et al. dat de open normen uit de artikelen 33 en 34 Wbp tot interpretatiemoeilijkheden leiden.

De verantwoordelijke moet de betrokkene informeren om de gegevensverwerking als rechtmatig aan te kunnen merken, maar ook omwille van de zorgvuldigheid die de verantwoordelijke ten opzichte van de betrokkene in acht heeft te nemen. De informatieplicht is immers een uitwerking van het in artikel 6 Wbp neergelegde ‘fair processing’ beginsel, alsook van het transparantiebeginsel. Dit transparantiebeginsel wordt benoemd in de overwegingen in de Privacyrichtlijn, maar is niet expliciet opgenomen in de bepalingen van de Privacyrichtlijn en de Wbp.

De adviescommissie Veiligheid en persoonlijke levenssfeer (Commissie Brouwer-Korf), het Cbp en de WRR benadrukken de noodzaak van transparantie. De betrokkene moet weten wie, waarom, waar en welke gegevens over hem verzamelt en gebruikt. De Commissie Brouwer-Korf concludeert dat, gezien de ontwikkelingen van technologie, de informatieplicht uit de Wbp niet langer een voldoende waarborg kan bieden, met als gevolg dat er slechts zicht bestaat op wat er in eerste instantie met de gegevens gebeurt maar niet wat opeenvolgende organisaties ermee doen. Op Europees niveau hebben zowel de Groep Gegevensbescherming Artikel 29, het EDPS als de Europese Commissie zich uitgelaten over transparantie. Het EDPS is onder meer van mening dat de artikelen 10 en 11 uit de Privacyrichtlijn moeten worden aangescherpt, en wel dusdanig dat de verantwoordelijke verplicht wordt om de informatie op een duidelijke, opvallende en begrijpelijke wijze te verstrekken. De Europese Commissie en de Groep Gegevensbescherming Artikel 29 expliciteren dat de bestaande bepalingen betreffende de aan de betrokkene te verstrekken informatie niet toereikend zijn. De Europese Commissie overweegt daarom een algemeen beginsel van transparante verwerking van persoonsgegevens op te nemen in de te herziene Privacyrichtlijn. Ook het kabinet heeft bij meerdere gelegenheden stilgestaan bij het belang van transparantie, maar ziet geen reden om de algemene formulering van de artikelen 33 en 34 Wbp te herzien. Dit geldt volgens het kabinet ook ten aanzien van de rechten van inzage, correctie en verzet. Wel is het kabinet voornemens om de verantwoordelijke te verplichten de vastgestelde bewaartermijnen bekend te maken en te verduidelijken wat er na afloop van

die termijn gebeurt met de verwerkte persoonsgegevens. Tevens overweegt het kabinet een afzonderlijke regeling te introduceren met specifieke transparantieverplichtingen bij het toepassen van profileringen, met inbegrip van een explicitering van het doel van de verwerking en de daarbij gehanteerde categoriseringen.

In de Nederlandse literatuur is meermaals opgemerkt dat de verantwoordelijke een privacyverklaring gebruikt om te voldoen aan zijn informatieplicht zoals die volgt uit de artikelen 33 en 34 Wbp. Daarbij kan de privacyverklaring ook een rol spelen bij het voldoen aan de informatieplichten die gelden voor de inzet van cookies. Relevant daarbij is dat de Groep Gegevensbescherming Artikel 29 van mening is dat cruciale informatie over het gebruik van cookies niet mag worden verstopt in een privacyverklaring.[274] Dit betekent dat het enkele gebruik van een privacyverklaring niet afdoende zal zijn bij het informeren van de betrokkene over het gebruik van cookies.
De Groep Gegevensbescherming Artikel 29 heeft een lijst opgesteld van elementen die minimaal in een privacyverklaring aan de orde zouden moeten komen. Er is een aantal argumenten dat lijkt te pleiten voor het nader uitwerken van de open normen van artikel 33 en 34 Wbp zoals wordt gedaan door de Groep Gegevensbescherming Artikel 29. Ten eerste zou men zich op grond van het transparantiebeginsel op het standpunt kunnen stellen dat de door de verantwoordelijke nader te verstrekken informatie zo uitgebreid als mogelijk dient te zijn, en dat derhalve ten aanzien van de inhoud van een privacyverklaring niet kan worden volstaan met het eenvoudig herhalen van een aantal wettelijke bepalingen uit de Wbp of slechts kan worden volstaan met de mededeling dat de verwerking van de persoonsgegevens plaatsvindt conform de Wbp.[275] Het voorgaande is te meer van belang nu er in de MvT op wordt gewezen dat de bedreiging van de persoonlijke levenssfeer in de informatiemaatschappij juist bestaat uit de vele mogelijkheden om persoonsgegevens buiten medeweten van de betrokkene om te verwerken.[276] Door de opname van zoveel mogelijk relevante informatie omtrent de verwerking van de persoonsgegevens in een privacyverklaring wordt de in de MvT gesignaleerde bedreiging geadresseerd. Zwenne et al. stellen in dit kader dat de positie van de betrokkene ten opzichte van de verantwoordelijke afhangt van de bekendheid van de betrokkene met de gegevens die de verantwoordelijke over hem verwerkt.[277] Ten tweede schept een lijst van op te nemen elementen meer duidelijkheid voor de verantwoordelijke. Hij hoeft in dat geval nagenoeg zijn hoofd niet meer ‘te breken’ over de vraag welke elementen hij in zijn privacyverklaring dient op te nemen en uit te werken ter waarborging van een behoorlijke en zorgvuldige verwerking jegens de

274 Groep Gegevensbescherming Artikel 29-2010 (I), p. 21.
275 Eenzelfde stelling wordt in de MvT gebezigd ten aanzien van gedragscodes die worden opgesteld op grond van artikel 25 Wbp. Kamerstukken II 1997-1998, 25892, nr. 3, p. 130.
276 Kamerstukken II 1997-1998, 25892, nr. 3, p. 18.
277 Zwenne et al., p. 48.

betrokkene.[278] Ten derde wordt voor de betrokkene een meer transparante situatie gecreëerd waardoor hij een beter zicht krijgt op de verwerkingshandelingen, aan de hand waarvan hij weet welke persoonsgegevens van hem door de verantwoordelijke worden verwerkt alsook op welke wijze zijn persoonlijke levenssfeer door de verantwoordelijke al dan niet wordt beschermd en gewaarborgd.
Tevens spreekt de Groep een voorkeur uit voor het gebruik van gelaagde privacyverklaringen. Het advies van de Groep Gegevensbescherming Artikel 29 is overigens niet bindend, wat een relevante constatering is nu de lijst veel elementen bevat waarvan onduidelijk is of die op grond van de artikelen 33 en 34 Wbp wel verplicht moeten worden verstrekt. In de Richtsnoeren Persoonsgegevens op internet conformeert het Cbp zich aan de adviezen van de Groep Gegevensbescherming Artikel 29, en geeft een voorbeeld van een privacyverklaring. Ook in dezen is het niet duidelijk of die Richtsnoeren juridisch bindend zijn voor de verantwoordelijke. Het komt er in de praktijk derhalve op neer dat de verantwoordelijke zelf dient te beslissen of hij een privacyverklaring op zijn website plaatst, alsook over de vorm en inhoud van de privacyverklaring. Indien de verantwoordelijke lid is van een belangenorganisatie, kan het voorkomen dat de verantwoordelijke op grond van het lidmaatschap verplichtingen opgelegd krijgt ten aanzien van het gebruik van een privacyverklaring.

Op basis van het in dit hoofdstuk uitgevoerde literatuuronderzoek kan ten eerste worden geconcludeerd dat de roep om transparantie in relatie tot de verwerking van persoonsgegevens steeds luider wordt. Ten tweede kan worden vastgesteld dat, beredenerend vanuit het belang van transparantie, de huidige bepalingen in de Privacyrichtlijn en de Wbp betreffende de aan de betrokkene te verstrekken informatie niet toereikend zijn. Derhalve zal, naar verwachting, in de herziene Privacyrichtlijn het transparantiebeginsel worden geëxpliciteerd. Ten slotte kan worden geconcludeerd dat een privacyverklaring een instrument is met behulp waarvan de verantwoordelijke kan voldoen aan zijn informatieplicht, en waarvan de inhoud de uitwerking van die informatieplicht concretiseert.

[278] De Groep Gegevensbescherming Artikel 29 wijst er mijns inziens terecht op dat met het verstrekken van de minimale informatie, de verantwoordelijke niet wordt ontslagen van de voor de verwerking geldende verplichting om de rechtmatigheid van de verwerking te controleren en na te gaan of deze voldoet aan het volledige pakket aan eisen en voorwaarden dat de toepasselijke nationale wetgeving voorschrijft. Groep Gegevensbescherming Artikel 29-2001, p. 3.

Hoofdstuk 3 | De privacyverklaring als overeenkomst

3.1 Inleiding

De privacyverklaring is in hoofdstuk 2 geanalyseerd vanuit het perspectief van de Wbp. Hieruit volgde dat de privacyverklaring een instrument is waarmee de verantwoordelijke kan voldoen aan zijn informatieplicht, en waarvan de inhoud de uitwerking van die informatieplicht concretiseert. De door de verantwoordelijke te verstrekken informatie is niet vrijblijvend van aard. De betrokkene moet ervan uit kunnen gaan dat de informatie correct is, en dat de verantwoordelijke zich houdt aan hetgeen hij in de privacyverklaring heeft verklaard. Met andere woorden, de verantwoordelijke neemt op grond van de privacyverklaring verplichtingen op zich die hij jegens de betrokkene moet nakomen.
De privacyverklaring kan echter ook breder worden toegepast dan uitsluitend als instrument ter concretisering van de informatieplicht uit de Wbp. De verantwoordelijke en de betrokkene kunnen immers afspraken maken die weliswaar zien op of gerelateerd zijn aan de verwerking van persoonsgegevens, maar die op grond van de Wbp niet hoeven te worden opgenomen in een privacyverklaring. Kijkend vanuit het perspectief van het Burgerlijk Wetboek (BW) zou een privacyverklaring mogelijk zijn te kwalificeren als een overeenkomst tussen de verantwoordelijke en de betrokkene.[279]

In dit hoofdstuk wordt de privacyverklaring vanuit een privaatrechtelijk perspectief geanalyseerd en wordt allereerst onderzocht of de verantwoordelijke en de betrokkene een overeenkomst kunnen sluiten met betrekking tot de verwerking van persoonsgegevens, en zo ja, of en in hoeverre zij daarin worden beperkt door de Wbp (paragrafen 3.2 en 3.3).[280] Aan de hand daarvan kan worden bepaald of de verantwoordelijke en de betrokkene in een privaatrechtelijke relatie, namelijk door middel van een privacyovereenkomst, de informatieplicht nader kunnen uitwerken. In paragraaf 3.4 zal het wettelijk kader voor elektronisch contracteren worden besproken, waarna in paragraaf 3.5 aandacht zal worden besteed aan de wijze waarop een privacyovereenkomst op elektronische wijze tot stand kan komen. In de paragrafen 3.6 en 3.7 worden de (rechts)maatregelen besproken die de

279 Vail et al. stellen dat een privacyverklaring als het ware dient te worden beschouwd als een contract tussen de onderneming die een website exploiteert en de consument. “Though not always true in practice, privacy policies are supposed to reflect a Web site’s actual privacy practices and serveas a contract between the Web site and the consumer”. Vail et al., p. 443. Ook indien met behulp van de zoekmachine Google wordt gezocht op het woord ‘privacyovereenkomst’ worden tientallen links getoond met verwijzingen naar websites die een privacyovereenkomst hebben. Zie bijvoorbeeld: https://www.metropolitanpanel.nl/MediaServer/Shared/documents/Netherlands%20-%20Privacy%20Policy.pdf; http://www.simview.nl/privacy.html; http://www.bsdevlieger.nl/fileadmin/beheerders/Download_documenten/privacyovereenkomst.pdf; http://www.trivianet.nl/help/privacy.php; http://www.jetairfly.com/privacy/nl/.

280 Zie in dit kader Berkvens, die opmerkt dat de wereld van databescherming niet goed aansluit bij de wereld van de gewone rechtspraak. Berkvens 2009-b, p. 102.

betrokkene kan treffen indien de verantwoordelijke zijn verplichtingen uit de privacyovereenkomst niet nakomt. Ook wordt bezien in hoeverre de betrokkene in dat geval schadevergoeding kan vorderen (paragraaf 3.8). In paragraaf 3.9 zal worden onderzocht of een privacyverklaring die wordt verstrekt in de vorm van een hyperlink kan worden gekwalificeerd als elektronische algemene voorwaarden zoals bedoeld in artikel 6:231 BW. Dit hoofdstuk wordt in paragraaf 3.10 afgesloten met een samenvatting en conclusies.

Bij de analyses geldt als vertrekpunt de situatie waarin de betrokkene via de website van de verantwoordelijke een dienst of product afneemt. Voorts wordt ervan uitgegaan dat de verantwoordelijke en de betrokkene in een overeenkomst afspraken willen maken over de verwerking van persoonsgegevens in relatie tot het afnemen van een product of dienst. De verantwoordelijke en de betrokkene beogen derhalve twee overeenkomsten tot stand te brengen: de overeenkomst die ziet op de levering van producten en/of diensten (hoofdovereenkomst) alsmede de privacyovereenkomst. De privacyovereenkomst is accessoir aan de hoofdovereenkomst. Door te kiezen voor deze opzet kan beter worden verduidelijkt op welke wijze een privacyovereenkomst tot stand kan komen en welke (rechts)maatregelen de betrokkene toekomen indien de verantwoordelijke zijn verplichtingen uit de beoogde overeenkomsten niet nakomt.[281] Hierop vooruitlopend kan worden vermeld dat de verantwoordelijke, naast de informatieplicht die volgt uit de Wbp, tevens een informatieplicht heeft die volgt uit het BW. Zoals in paragrafen 3.6.2 en 3.7.1. zal blijken, verkrijgt de betrokkene additionele mogelijkheden om de privacyovereenkomst te ontbinden of te vernietigen indien de verantwoordelijke deze informatieplicht niet naleeft.

3.2 De toelaatbaarheid van een overeenkomst die ziet op de verwerking van persoonsgegevens

De eerste vraag die moet worden beantwoord is of de verantwoordelijke en de betrokkene in een overeenkomst afspraken kunnen maken met betrekking tot de verwerking van persoonsgegevens. Naar de mening van Cuijpers kunnen de verantwoordelijke en de betrokkene in een overeenkomst, en in afwijking van de Privacyrichtlijn, afspraken maken over de wijze waarop persoonsgegevens worden verwerkt. “In my opinion, Directive 95/46/EC does not require implementation into mandatory rules of law. Instead, the directive offers a framework on how to process personal data when there is no contractual relationship, or when the contract does not concern the processing of personal data, even

[281] Men zou bijvoorbeeld ook kunnen kiezen voor de constructie dat er een overeenkomst tot stand komt, waarbij de inhoud van de privacyverklaring een onlosmakelijk deel vormt van die overeenkomst.

though processing of these data forms part of the relationship. Therefore, it is possible to deviate from the rules laid down in Directive 95/46/EC on the basis of a contract".[282]
Purtova daarentegen weerlegt de argumenten van Cuijpers en komt tot de conclusie dat partijen niet mogen afwijken van het regime van de Privacyrichtlijn. "Therefore, the provisions of the Directive, e.g. establishing the data subject's rights, cannot be 'contracted around' with effect of the contract taking precedence over those rights".[283] De argumenten die door Cuijpers en Purtova in ogenschouw worden genomen zien op de harmonisering van regelgeving binnen de Europese Unie, het ontbreken van een bepaling in de Privacyrichtlijn waaruit zou volgen dat er niet bij overeenkomst kan worden afgeweken van die richtlijn, het beginsel van contractsvrijheid, economische motieven en het beschermingsniveau dat onder meer door het BW wordt geboden ten aanzien van de bescherming van persoonsgegevens.

Cuijpers: "Harmonisation of the rules is only necessary for those instances in which nothing is agreed amongst the data controller and the data subject themselves, and, because of this lack of agreement, the respective national laws governing the processing of personal data interfere with the desired transaction". "Even though this judgement broadens the authority to harmonise on the basis of article 100A to a large extent, it also reveals that harmonisation is only possible in view of the free movement of data, and not (solely) in view of the protection of a fundamental right".[284]
Purtova: "The main disagreement between the position of this book and the 'free market argument' lies in our understanding of the 'internal market'".[285] "The overall conclusion is that Cuijpers' comprehension of the 'internal market' as a free market is contrary to the established understanding thereof. Similarly, the free movement of data does not mean the data flows must be free of state regulation".[286]

Cuijpers: "Therefore, the absence of a clause requiring the mandatory character of one or more of the provisions laid down in Directive 95/46/EC, supports the view that the directive does not require implementation law with a mandatory character".[287] "Even though governments cannot implement rules that deviate from the provisions laid down in the directive, this does not mean that data controllers and data subjects cannot deviate from the implemented rules. The situation is different if a directive explicitly requires implementation into mandatory rules of national law."[288] "The second remark concerns article 7 of

282 Cuijpers 2007, p. 306.
283 Purtova, p. 209.
284 Cuijpers 2007, p. 308 e.v.
285 Purtova, p. 197.
286 Purtova, p. 198.
287 Cuijpers 2007, p. 310 e.v.
288 Cuijpers 2007, p. 310.

Directive 95/46/EC. This article explicitly leaves room to process personal data on a contractual basis, or with the consent of the data subject. Moreover, the directive expressly states the advantages of self-regulation".[289]
Purtova: "As a result, although the 1995 Directive is not directly binding on private entities, these parties are not immune to the substance of its data protection requirements".[290] "The 1995 Directive provides for the rights of data subjects and imposes obligations on data controllers. There is, therefore no doubt that it applies to private parties, albeit through state action".[291]

Cuijpers: "Even if the right is considered to be rooted in a fundamental right, there still is no solid argument to hierarchically place data protection above the principle of freedom of contract, leaving room for implementation of Directive 95/46/EC into rules of a regulatory nature".[292]
Purtova: "Nothing suggests that the freedom of contract should take precedence over data protection interests. Instead, a fair balance between data protection and other interests, including the freedom of contract, must be achieved".[293]

Cuijpers: "From an economic perspective, the desirability of mandatory rules of law concerning the processing of personal data is therefore doubtful".[294]
Purtova: "…the fact that the Directive does indeed take some data protection issues off the agenda for negotiation means that while some actors may wish that the situation was different, it is not".[295] "It is hard to dispute the fact that the imposition of any mandatory rules of law limits both the scope of rights and the contractual freedom of the participants to a transaction. Nevertheless, it would be wrong to assert that the limitations imposed on negotiations by Directive 95/46/EC are unreasonable".[296]

Cuijpers: "The norms limiting the freedom of contract mentioned above all lead to the conclusion that, on the basis of Dutch law of obligations, the same result will often be reached as specifically prescribed by Directive 95/46/EC for the processing of personal data. Analysis of this law shows that it only seldom permits deviation from the rules that are laid down by the directive. Thus, also in practice there is no need for implementation of Directive 95/46/EC into mandatory rules of law".[297]

289 Cuijpers 2007, p. 311.
290 Purtova, p. 200.
291 Purtova, p. 201.
292 Cuijpers 2007, p. 314.
293 Purtova, p. 203.
294 Cuijpers 2007, p. 315.
295 Purtova, p. 204.
296 Purtova, p. 204.
297 Cuijpers 2007, p. 316.

> Purtova: "To summarize, whereas data protection can indeed benefit from the mechanisms of contract and consumer protection law, this fact alone is not enough to call for the use of these instruments as completely independent alternatives to the rules of the Directive".[298]

Volgens Purtova is het wel mogelijk dat de verantwoordelijke en de betrokkene aangaande de verwerking van persoonsgegevens een overeenkomst afsluiten die *in lijn* is met de Privacyrichtlijn: "…when implementing the Directive's provisions, member states may also leave room for contracts to be made in the field of data processing, but only within the framework of the Directive".[299] Kijkend naar de Wbp, stelt de MvT dat de voorschriften van de Wbp worden gekwalificeerd als dwingend recht. "De kwalificatie van de Wbp als dwingend recht heeft tot gevolg dat een rechtshandeling waarbij afstand wordt gedaan van de door de Wbp toegekende rechten in beginsel wegens strijd met de openbare orde nietig is op grond van artikel 3:40 van het Burgerlijk Wetboek".[300] Hieruit kan worden opgemaakt dat de verantwoordelijke en de betrokkene in een privacyovereenkomst afspraken kunnen maken over de verwerking van persoonsgegevens op voorwaarde dat er geen afstand wordt gedaan van de rechten en verplichtingen die worden toegekend op grond van de Wbp. Kortom, dat zij met hun contractuele afspraken binnen de kaders van de Wbp blijven. Van der Sloot tekent in dezen aan dat "de contractsvrijheid in een privaatrechtelijk beschermingsmodel van privacy altijd wordt beperkt door contractuele beperkingen die nietigheid bewerkstelligen, zoals bepalingen die tegen het in het maatschappelijk verkeer betamelijke indruisen".[301] Cuijpers et al. expliciteren dat "overeenkomsten op diverse wijzen een rol spelen bij het invullen of onderbouwen van de normstelling van de Wbp, en dat deze een zeer relevant instrument vormen bij het concretiseren van de beoogde wettelijke privacybescherming".[302] Hoving stelt dat de informatieplicht *an sich* geen object van een overeenkomst kan zijn, maar meent dat het wel mogelijk is om een privacyovereenkomst accessoir te maken aan een overeenkomst die ziet op het leveren van producten of diensten.[303]

---

298 Purtova, p. 208.

299 Purtova, p. 199. Zo ook Cuijpers et al., p. 37.

300 Kamerstukken II 1997-1998, 25892, nr. 3, p. 10. Zie ook Van der Sloot 2010, p. 107.

301 Van der Sloot 2011-b, p. 233.

302 Cuijpers et al., p. 36 e.v. Zij noemen als voorbeeld een bewerkersovereenkomst of een overeenkomst waarin (praktische) afspraken worden gemaakt over de wijze waarop bepaalde wettelijke rechten van de betrokkene kunnen worden uitgeoefend.

303 Volgens Hoving neemt het BW als uitgangspunt dat alleen bij die rechtsplichten waarmee een subjectief vermogensrecht correspondeert van degene jegens wie de rechtsplicht bestaat wordt gesproken van verbintenissen. In haar analyse stelt Hoving dat de informatieplicht van de verantwoordelijke niet vatbaar is voor overdracht, dat de informatieplicht niet gericht is om stoffelijk voordeel aan de betrokkene te verschaffen en dat het tevens geen deel uit maakt van diens (verhandelbare) vermogen. Zij komt daarmee tot de conclusie dat de informatieplicht geen vermogensrecht is in de zin van Boek 6 BW, en om deze reden geen object van een overeenkomst kan zijn. Daarbij stelt Hoving dat met de informatieplicht van de verantwoordelijke geen subjectief vermogensrecht correspondeert dat deel uitmaakt van het vermogen van de betrokkene. Hoving, p. 128 e.v.

In navolging van de opvattingen van Cuijpers als Purtova stel ik vast dat de verantwoordelijke en de betrokkene een overeenkomst met elkaar kunnen aangaan met betrekking tot de verwerking van persoonsgegevens, zolang de inhoud van de overeenkomst niet in strijd is met het minimumbeschermingsniveau zoals neergelegd in de Privacyrichtlijn en de Wbp. In aanvulling hierop wordt de contractsvrijheid van de verantwoordelijke en de betrokkene beperkt door het BW, in het bijzonder artikel 3:40 BW. Concluderend betekent het voorgaande dat de verantwoordelijke en de betrokkene de informatieplicht, en daarmee de open normen, uit artikel 33 en 34 Wbp nader kunnen concretiseren aan de hand van het instrument privacyovereenkomst. Ten aanzien van de inhoud en strekking van deze overeenkomst gelden de beperkingen uit de Wbp en het BW.

3.3 De inhoud van de privacyovereenkomst

In paragraaf 2.3.2 zijn de elementen benoemd die volgens de Groep Gegevensbescherming Artikel 29 zouden moeten worden opgenomen in een privacyverklaring. Met betrekking tot deze elementen is in hoofdstuk 2 geconcludeerd dat niet duidelijk is of op grond van de artikelen 33 en 34 Wbp alle door de Groep genoemde elementen verplicht moeten worden opgenomen in een privacyverklaring. Ten aanzien van de elementen 'identiteit van de verantwoordelijke' en 'het doel van de verwerking' bestaat die onduidelijkheid niet. Deze dienen op grond van de artikelen 33 en 34 Wbp te worden vermeld. De verantwoordelijke en de betrokkene zouden ten aanzien van de inhoud van de privacyovereenkomst de lijst van de Groep Gegevensbescherming Artikel 29 als leidraad kunnen nemen, dan wel zich hieraan volledig conformeren. In de praktijk blijft vanwege de open normen van de artikelen 33 en 34 Wbp rechtsonzekerheid bestaan of de betreffende inhoud van de privacyovereenkomst voldoende is om ten aanzien van een specifiek geval te hebben voldaan aan de informatieplicht van de Wbp.

De Wbp kent zes grondslagen op basis waarvan de verantwoordelijke persoonsgegevens kan verwerken.[304] De grondslagen staan genoemd in artikel 8 Wbp.

> Artikel 8 Wbp
> Persoonsgegevens mogen slechts worden verwerkt indien:
> a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;

[304] Berkvens pleit ervoor de (herziene) regelgeving van het databeschermingsrecht meer te gaan toepassen op 'degene die persoonsgegevens verwerkt'. Dienaangaande geeft hij ter overweging om artikel 7 Privacyrichtlijn (zoals vervat in het huidige artikel 8 Wbp) uit te breiden met een onderdeel g: 'Persoonsgegevens mogen slechts worden verwerkt indien: g. de verwerking noodzakelijk is in het kader van een met een derde afgesloten overeenkomst'. Berkvens 2011, p. 262.

b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Kijkend naar de inhoud van de privacyovereenkomst is allereerst artikel 8 sub a Wbp relevant. Dit artikel bepaalt dat persoonsgegevens slechts mogen worden verwerkt indien de betrokkene voor de verwerking zijn 'ondubbelzinnige toestemming' heeft verleend.[305] In de privacyovereenkomst kunnen de verantwoordelijke en de betrokkene vastleggen ten aanzien van welke verwerkingen de betrokkene zijn ondubbelzinnige toestemming heeft gegeven. De betrokkene kan er tevens voor kiezen om aan de hand van de privacyovereenkomst zijn ondubbelzinnige toestemming te verstrekken.[306] Voor de rechtsgeldigheid van de ondubbelzinnige toestemming is het wel noodzakelijk dat alle voor de verwerking relevante informatie op een transparante wijze wordt opgenomen in de privacyverklaring. "A second dimension of consent relates to information: transparency towards the data subject. Transparency is a condition of being in control and for rendering the consent valid. Transparency as such is not enough to legitimise the processing of personal data, but it is an essential condition in ensuring that consent is valid. To be valid, consent must be informed. This implies that all the necessary information must be given at the moment the consent is requested, and that this should address the substantive aspects

305 In paragraaf 2.2.2.1 is verduidelijkt wat onder ondubbelzinnige toestemming wordt verstaan.

306 Dit geldt evenzo voor de gevallen waarin de betrokkene zijn 'uitdrukkelijke toestemming' heeft gegeven of wil geven ten aanzien van de verwerking van bijzondere gegevens conform artikel 23 lid 1 sub a Wbp. Het verwerken van bijzondere persoonsgegevens zoals over godsdienst, gezondheid of politieke gezindheid is niet toegestaan op grond van artikel 16 Wbp, tenzij de betrokkene conform artikel 23 lid 1 sub a Wbp zijn uitdrukkelijke toestemming hiervoor heeft gegeven. "Bij de verplichting tot een uitdrukkelijke toestemming van de betrokkene, dient de betrokkene expliciet zijn wil omtrent de verwerking te hebben geuit aan de verantwoordelijke. Een stilzwijgende of impliciete toestemming is onvoldoende: de betrokkene dient in woord, schrift of gedrag uitdrukking te hebben gegeven aan zijn wil toestemming te verlenen aan de hem betreffende gegevensverwerking". Hooghiemstra & Nouwt, p. 124, aant. 111.

of the processing that the consent is intended to legitimise. This would normally cover the elements of information listed in Article 10 of the Directive, but will also depend on when, and the circumstances in which, consent is requested".[307] Daarbij dient te worden aangetekend dat artikel 8 sub a Wbp spreekt van 'toestemming' en niet van 'overeenkomst'. Cuijpers merkt hierover op dat in het Nederlandse privaatrecht enkel in theorie een onderscheid tussen toestemming en contract bestaat. "Alle rechtshandelingen worden in Nederland echter beheerst door dezelfde regels inzake totstandkoming, geldigheid en nietigheid, waardoor er praktisch geen verschillen bestaan".[308] In dit kader is tevens relevant de visie van de Groep Gegevensbescherming Artikel 29 die stelt dat 'toestemming' en het overeenkomstenrecht ten opzichte van elkaar aanvullend zijn. "Consent is also a notion used in other fields of law, particularly contract law. In this context, to ensure a contract is valid, other criteria than those mentioned in the Directive will be taken into account, such as age, undue influence, etc. There is no contradiction, but an overlap, between the scope of civil law and the scope of the Directive: the Directive does not address the general conditions of the validity of consent in a civil law context, but it does not exclude them".[309]

De verantwoordelijke kan in een privacyovereenkomst verplichtingen op zich nemen die verder gaan dan de verplichtingen die voor hem voortvloeien uit de Wbp.[310] De verantwoordelijke kan bijvoorbeeld verduidelijken op basis van welke grondslag (of grondslagen), naast de grondslag van artikel sub a Wbp, hij persoonsgegevens verwerkt. Ook zou de verantwoordelijke kunnen verklaren dat hij nimmer persoonsgegevens aan derden zal verstrekken met het oog op werving voor commerciële doelen.[311] De verantwoordelijke zou ook in de privacyovereenkomst kunnen verduidelijken of er, en zo ja welke, verschillen zijn met betrekking tot verwerkingen in de precontractuele of contractuele fase. Tevens zou hij de organisatorische en technische maatregelen kunnen benoemen die door hem zijn getroffen ter bescherming van de persoonsgegevens. Evenzo kan de verantwoordelijke zich ertoe verplichten om de betrokkene te informeren mocht er sprake zijn van een datalek binnen zijn organisatie. Voorts biedt de privacyovereenkomst de mogelijkheid om de procedure te beschrijven die de verantwoordelijke in acht neemt ter controle op de naleving van de verplichtingen die hij op grond van de Wbp en de

307 Groep Gegevensbescherming Artikel 29-2011, p. 9. In hoofdstuk 5 zal het belang van transparantie nader aan de orde komen.

308 Cuijpers 2004, p. 159. Vergelijk Purtova, p. 191 e.v.

309 Groep Gegevensbescherming Artikel 29-2011, p. 6.

310 Vergelijk Verkade die in het kader van een gedragscode zoals bedoeld in artikel 25 Wbp stelt: "Wat in deze statusdiagnose verder op te merken valt, is dat een 'verantwoordelijke' die in zijn contractuele betrekking met een cliënt naar een gedragscode verwijst, daaraan contractueel gehouden kan worden, ook als zijn verplichtingen daarmee verder zouden gaan dan uit de Wbp zelf zou voortvloeien. Het omgekeerde stuit mijns inziens af op het gegeven dat de bepalingen van de Wbp naar hun aard in die zin dwingend zijn dat daarvan niet ten nadele van de 'betrokkene' (de geregistreerde persoon) kan worden afgeweken". Verkade, punt 4.14. Zie in dit kader tevens Siemerink et al, p. 143.

311 Zie artikel 41 Wbp.

privacyovereenkomst heeft. De verantwoordelijke en de betrokkene kunnen een boetebeding overeenkomen, zodat de betrokkene geen gerechtelijke procedure hoeft te starten indien de verantwoordelijke persoonsgegevens verwerkt in strijd met de Wbp of de privacyovereenkomst. Maar niet alleen de verantwoordelijke kan aan de hand van de privacyovereenkomst verplichtingen op zich nemen. Zo kan de betrokkene de verplichting op zich nemen om de juiste en volledige persoonsgegevens aan de verantwoordelijke te verstrekken.[312] Tevens zou de betrokkene zich kunnen verplichten om eventuele wijzigingen ten aanzien van zijn persoonsgegevens door te geven aan de verantwoordelijke.

3.4 Wettelijk kader voor elektronisch contracteren

In de inleiding van dit hoofdstuk is als uitgangspunt genomen dat de verantwoordelijke en de betrokkene zowel de overeenkomst die ziet op de levering van producten en/of diensten als de privacyovereenkomst langs digitale weg tot stand brengen. Anders gezegd, er is sprake van elektronisch contracteren, waarbij onder elektronisch contracteren wordt verstaan het sluiten van overeenkomsten waarbij het aanbod en de aanvaarding plaatsvindt door middel van het gebruik van elektronische middelen. Het wettelijk kader voor het elektronisch contracteren is neergelegd in een aantal Europese richtlijnen en de implementatie daarvan in het Nederlands recht. Als belangrijkste worden hier genoemd de Europese richtlijn Overeenkomsten op afstand[313], de Europese richtlijn Elektronische handtekeningen[314] en de Europese richtlijn Elektronische handel.[315] De laatstgenoemde richtlijn heeft als doel het

312 Het is algemeen bekend feit dat een betrokkene veelal de datum 11-11-11 invult als zijnde zijn geboortedatum.

313 Richtlijn 97/7/EG van het Europees Parlement en de Raad van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten (PbEG L 144). De implementatie van deze richtlijn in het Nederlands recht heeft plaatsgevonden bij Wet van 21 december 2000, houdende aanpassing van Boek 7 van het Burgerlijk Wetboek aan richtlijn nr. 97/7/EG van het Europees Parlement en de Raad van de Europese Unie van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten (PbEG L 144), Stb. 2000, 617.

314 Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 013). De implementatie van deze richtlijn in het Nederlands recht heeft plaatsgevonden bij Wet van 8 mei 2003 tot aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13) (Wet elektronische handtekeningen), Stb. 2003, 199.

315 Richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PbEG L 178). De implementatie van deze richtlijn in het Nederlands recht heeft plaatsgevonden bij Wet van 13 mei 2004 tot aanpassing van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht en de Wet op de economische delicten ter uitvoering van richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de

scheppen van een juridisch kader teneinde het vrije verkeer van diensten van de informatiemaatschappij te waarborgen.[316] In die richtlijn, alsook in een aantal bepalingen dat ter implementatie van de richtlijn is opgenomen in het BW[317,] wordt gesproken over de 'dienstverlener' en 'diensten van de informatiemaatschappij'. Uit artikel 3:15d lid 3 BW volgt dat onder dienst van de informatiemaatschappij wordt verstaan elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn. Dit artikel bepaalt tevens dat een dienst langs elektronische weg wordt verricht indien deze geheel per draad, per radio, of door middel van optische of andere elektromagnetische middelen wordt verzonden, doorgeleid en ontvangen met behulp van elektronische apparatuur voor de verwerking, met inbegrip van digitale compressie, en de opslag van gegevens. De essentie van het elektronisch contracteren is er kortom in gelegen dat de overeenkomst zelf geheel langs elektronische weg tot stand komt, en niet of er elektronische apparatuur bij de totstandkoming van de overeenkomst is gebruikt.[318]

Doordat de wetgever expliciet de termen 'dienstverlener' en 'dienst van de informatiemaatschappij' benoemt, suggereert hij dat de bepalingen die hierop betrekking hebben niet van toepassing zouden zijn op de verkoper die online producten verkoopt. In de Europese richtlijn Elektronische handel wordt overwogen dat onder dienst van de informatiemaatschappij ook activiteiten vallen die bestaan in de on-lineverkoop van goederen, maar dat de *levering* van goederen *als zodanig* of de verstrekking van off-linediensten niet onder de richtlijn vallen.[319] Ook de MvT van de Aanpassingswet Richtlijn inzake Elektronische handel maakt duidelijk dat onder dienst van de informatiemaatschappij mede online verkopen dient te worden verstaan.[320] Derhalve geldt dat zowel het online

---

interne markt (PbEG L 178) (Aanpassingswet richtlijn inzake elektronische handel), Stb. 2004, 210. De Aanpassingswet is op 30 juni 2004 in werking getreden op grond van het Besluit van 18 juni 2004, houdende vaststelling tijdstip van inwerkingtreding van de wet van 13 mei 2004 tot aanpassing van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht en de Wet op de economische delicten ter uitvoering van richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PbEG L 178) (Aanpassingswet richtlijn inzake elektronische handel) (Stb. 210), Stb. 2004, 285.

316 Uit overwegingen 7 en 8 van de richtlijn blijkt dat de richtlijn een duidelijk en algemeen kader wil bieden ter wille van de rechtszekerheid en het vertrouwen van de consument.

317 Zie bijvoorbeeld artikelen 3:15d tot en met 3:15f BW; artikel 6:227b BW.

318 Er is bijvoorbeeld geen sprake van elektronisch contracteren in geval van een feitelijke aflevering van een uitgeprint e-mailbericht.

319 Richtlijn inzake Elektronische Handel, overweging 18. Zie ook artikel 2 sub h.ii. van deze richtlijn.

320 De MvT verduidelijkt dit aan de hand van twee voorbeelden: 'Als een consument langs elektronische weg downloadbare muziek aanschaft, vinden zowel de totstandkoming van de koopovereenkomst als de levering langs elektronische weg plaats. Beide rechtshandelingen vallen daardoor onder het bereik van de richtlijn. Als dezelfde consument echter een boek langs elektronische weg aanschaft, en (af)levering daarvan feitelijk, bijvoorbeeld per post, plaatsvindt, is de richtlijn op deze, (af)levering niet van toepassing'. Kamerstukken II, 2001-2002, 28197, nr. 3, p. 24.

leveren van diensten als het online verkopen van goederen onder de definitie ‘dienst van de informatiemaatschappij’ valt.

De verantwoordelijke die aan de hand van zijn website diensten levert of producten verkoopt, levert derhalve een ‘dienst van de informatiemaatschappij’. Dit heeft tot gevolg dat de verantwoordelijke in beginsel moet voldoen aan de informatieplichten zoals die zijn opgenomen in de artikelen 3:15d BW, 3:15e BW en 6:227b BW.[321] Tevens dient de verantwoordelijke te voldoen aan de informatieplichten zoals benoemd in de artikelen 7:46a e.v. BW.[322] Het door de verantwoordelijke niet voldoen aan bepaalde informatieplichten geeft de betrokkene de mogelijkheid om een langs elektronische weg gesloten overeenkomst te ontbinden of te vernietigen.

3.5 De totstandkoming en naleving van de privacyovereenkomst

Ten aanzien van op elektronische wijze gesloten overeenkomsten geldt de ‘normale’ hoofdregel van artikel 6:217 lid 1 BW: een overeenkomst komt tot stand door een aanbod en de aanvaarding daarvan.[323] Holleman stelt dat een privacystatement een verklaring van de aanbieder van de website inhoudt over de wijze waarop hij omgaat met de persoonsgegevens. Deze verklaring is volgens Holleman niet vrijblijvend van aard, aangezien de aanbieder met die verklaring beoogt kenbaar te maken dat hij zich aan het door hem toegezegd gedrag zal houden, anders gezegd zich tot dat gedrag verplicht. “Een dergelijke verklaring is slechts niet vrijblijvend indien zij rechtens kan worden afgedwongen, en daarmee kan de privacystatement worden gekarakteriseerd als een verklaring met een beoogd rechtsgevolg. Het is derhalve een rechtshandeling zoals bedoeld in art. 3:33 BW, omdat het een op een rechtsgevolg gerichte wil bevat die zich door een verklaring heeft geopenbaard in de vorm van een aanbod”.[324] Verklaringen dienen om de wil van partijen te uiten. Daarbij tekende de Nota Wetgeving voor de elektronische snelweg in 1998 aan dat de wil in het elektronische rechtsverkeer dezelfde rol kan vervullen als in de huidige situatie, omdat het gaat om de geestesgesteldheid van degene die een bepaalde rechtshandeling wil verrichten, hetgeen uiteraard niet aan het gebruik van een bepaalde communicatietechniek is gebonden.[325] Een verklaring heeft werking vanaf het moment waarop zij degene, tot wie

---

321 In paragraaf 3.6.2 wordt duidelijk dat de informatieplicht die volgt uit artikel 6:227b BW niet in alle gevallen geheel of gedeeltelijk door de verantwoordelijke behoeft te worden nagekomen.

322 Deze informatieplichten zijn in Boek 7 opgenomen ter implementatie van de Europese richtlijn Overeenkomsten op afstand.

323 In dit onderzoek wordt ervan uitgegaan dat zowel het aanbod van de verantwoordelijke in de vorm van de privacyverklaring als de aanvaarding daarvan door de betrokkene op elektronische weg wordt uitgebracht.

324 Holleman 2005, p. 168.

325 Nota Wes, p. 59-60. Zie ook Van der Klaauw-Koops, p. 130 e.v.

zij gericht is, heeft bereikt, aldus artikel 3:37 lid 3 BW. Indien een verklaring niet tot een bepaald persoon gericht is, werkt deze verklaring reeds vanaf het moment der wilsuiting. Het aanbod van de verantwoordelijke geldt derhalve op het moment dat hij de privacyverklaring op zijn website plaatst.

Naar de opvatting van Holleman vindt aanvaarding van de privacyverklaring plaats zodra de betrokkene zijn persoonsgegevens intypt.[326] Het is echter de vraag of het verstrekken van persoonsgegevens wel mag worden opgevat als een aanvaarding van de privacyverklaring. In navolging van Van Esch en Blok ben ik echter van mening dat dit niet het geval is.[327] In zowel het BW als in de MvT van de Aanpassingswet Richtlijn inzake Elektronische handel wordt niet verduidelijkt welke feitelijke handeling(en) de betrokkene moet verrichten om een aanbod op elektronische wijze te aanvaarden. In de praktijk dient de betrokkene met betrekking tot een aankoop via een website veelal, na het bestelproces te hebben doorlopen, op een button te klikken.[328] In paragraaf 3.3 is reeds aangekaart dat een grondslag voor het mogen verwerken van persoonsgegevens is gelegen in het verstrekken van 'ondubbelzinnige toestemming'.[329] De Groep Gegevensbescherming stelt dat de betrokkene in een online omgeving zijn ondubbelzinnige toestemming kan geven via het aanvinken van een 'tick box' op de website van de verantwoordelijke.[330] Met betrekking tot de aanvaarding van de privacyverklaring, en daarmee de totstandkoming van de privacyovereenkomst, zouden de verantwoordelijke en de betrokkene mijns inziens de navolgende procedure moeten doorlopen:

1. De verantwoordelijke moet aan de betrokkene de mogelijkheid bieden om de privacyverklaring te kunnen lezen.
2. Onderaan de privacyverklaring is een 'tick box' weergegeven die de betrokkene dient aan te vinken waarmee hij verklaart dat hij de privacyovereenkomst heeft gelezen. Indien de betrokkene aan de hand van de privacyovereenkomst zijn ondubbelzinnige toestemming wil verlenen ten behoeve van een bepaalde verwerking, is het aan te bevelen dat de betrokkene tevens verklaart dat hij met het aanvinken van de tick box zijn ondubbelzinnige toestemming verstrekt ten aanzien van die verwerking.
3. Nadat de betrokkene de 'tick box' heeft aangevinkt, verschijnt er een button waarop hij dient te klikken indien hij de privacyovereenkomst wil aanvaarden.

---

326 Holleman 2005, p. 168.

327 Van Esch & Blok, p. 221.

328 De naamgeving aan de button is in de praktijk divers. Enkele voorbeelden zijn "bestel", "accepteer" en "klik hier voor de definitieve bestelling".

329 Respectievelijk artikel 8 sub a Wbp en artikel 23 lid 1 sub a Wbp.

330 Groep Gegevensbescherming Artikel 29-2011, p. 22. "Ticking the box after having received relevant information would constitute express, unambiguous consent as the action of ticking the box is clear enough to leave no doubt as to the individual's wish to be enrolled in the loyalty programme". Zie over het gebruik van een tick box bijvoorbeeld het arrest van het Gerechtshof 's-Hertogenbosch 22 maart 2011 (LJN: BP9625).

Hoewel deze aanvaardingsprocedure vanuit het perspectief van rechtszekerheid de ogenschijnlijk noodzakelijke waarborgen met zich mee brengt, blijft het de vraag of daarmee de aanvaarding vanuit juridisch oogpunt onaantastbaar wordt. De betrokkene verklaart weliswaar dat hij de privacyovereenkomst heeft gelezen, maar is dat ook feitelijk het geval? Het is algemeen bekend dat websitebezoekers veelal ter acceptatie van voorwaarden op een button klikken of een tick box aanvinken zonder die voorwaarden daadwerkelijk gelezen te hebben. Zelfs al zou de betrokkene in dit geval de privacyovereenkomst hebben gelezen, is het dan realistisch om te veronderstellen dat hij deze ook daadwerkelijk heeft begrepen? Anders gezegd, mag er van de betrokkene worden verwacht dat hij de omvang en consequenties overziet indien zijn persoonsgegevens worden verwerkt conform de privacyovereenkomst?[331] Aspecten als leesbaarheid en begrijpelijkheid van de privacyovereenkomst, die in feite neerkomen op de mate waarin transparantie richting de betrokkene wordt betracht, spelen daarbij een belangrijke rol.[332] De betrokkene zou zich in geval van een 'niet-leesbare' of 'niet-begrijpelijke' privacyovereenkomst mogelijk kunnen beroepen op dwaling.[333] De rechtsgeldigheid van de aanvaarding kan tevens worden betwist indien de verantwoordelijke de 'take it or leave it' methode hanteert. De betrokkene *moet* in dat geval de privacyverklaring aanvaarden, wil hij tot de aankoop van een product kunnen overgaan.

Op grond van artikel 3:37 lid 3 BW zou de privacyovereenkomst tussen de verantwoordelijke en betrokkene tot stand komen op het moment dat de verklaring van de betrokkene de verantwoordelijke heeft bereikt. Voor een aanvaarding – in vervolg op een via elektronische weg uitgebracht aanbod – die langs elektronische weg wordt uitgebracht geldt echter de bepaling van artikel 6:227c lid 3 BW. In dit artikel is bepaald dat een dergelijke aanvaarding wordt geacht te zijn ontvangen indien deze toegankelijk is voor de partij tot wie deze is gericht. De privacyovereenkomst tussen de verantwoordelijke en de betrokkene komt derhalve tot stand op het moment dat de verklaring van de betrokkene, zijnde de aanvaarding van het aanbod van de verantwoordelijke, toegankelijk is geworden voor de verantwoordelijke.

Holleman is van mening dat de privacyovereenkomst die tussen de verantwoordelijke en de betrokkene tot stand komt kan worden gekwalificeerd als een eenzijdige overeenkomst.[334] Dit is juist voor zover de betrokkene op grond van de privacyovereenkomst geen verplichtingen op zich heeft genomen.[335] Het begrip eenzijdige overeenkomst wordt niet in het BW als zodanig gedefinieerd maar kan worden afgeleid uit artikel 6:261 lid 1 BW dat ziet

331 Vergelijk Van der Sloot 2010, p. 108.
332 In hoofdstuk 5 komt dit aspect nader aan de orde.
333 In paragraaf 3.7.2 komt dit nader aan de orde.
334 Holleman 2005, p. 168.
335 Zie paragraaf 3.3.

op de wederkerige overeenkomst. Overeenkomsten die niet wederkerig zijn, zijn eenzijdig.[336] De kern van een wederkerige overeenkomst is gelegen in het ruilkarakter waarbij ieder van de betrokken partijen een verbintenis op zich neemt ter verkrijging van een prestatie die wordt geleverd door de andere partij.[337]

Indien de verantwoordelijke zijn verplichtingen uit hoofde van de privacyovereenkomst niet nakomt is sprake van een tekortkoming in de nakoming van de overeenkomst. De betrokkene heeft in dat geval de mogelijkheid op grond van artikel 3:296 lid 1 BW een vordering tot nakoming van de privacyovereenkomst in te stellen.[338] In de volgende paragrafen wordt besproken welke andere rechtsmaatregelen ter beschikking staan aan de betrokkene indien de verantwoordelijke zich niet houdt aan verplichtingen die hij door middel van de privacyovereenkomst op zich heeft genomen.[339] Daarbij dient te worden aangetekend dat de bespreking is gebaseerd op het strikt juridische regime, maar dat de feitelijke praktijk een heel andere realiteit kan tonen.

3.6 Ontbinding

In het onderstaande wordt allereerst geanalyseerd op welke gronden de betrokkene de privacyovereenkomst mogelijk kan ontbinden. In paragraaf 3.6.1 komt ontbinding op grond van artikel 6:265 BW aan de orde. Vervolgens wordt in paragraaf 3.6.2. onderzocht of de betrokkene de privacyovereenkomst kan ontbinden indien de verantwoordelijke bepaalde informatieplichten uit het BW niet naleeft. In paragraaf 3.6.3 zal blijken dat de betrokkene de privacyovereenkomst kan ontbinden zolang de verantwoordelijke geen bevestiging aan hem heeft verzonden in vervolg op de aanvaarding van de privacyovereenkomst. Ten slotte worden in paragraaf 3.6.4 de gevolgen voor de privacyovereenkomst in ogenschouw genomen indien de betrokkene een eerder door hem verstrekt ondubbelzinnige toestemming intrekt.

3.6.1 Ontbinding op grond van artikel 6:265 BW

Indien de verantwoordelijke de plichten uit de privacyovereenkomst niet nakomt heeft de betrokkene de mogelijkheid om de privacyovereenkomst te ontbinden op grond van het

336 Zie ook Asser/Hartkamp/Sieburgh, nr. 82. Zo ook Hijma & Olthof, p. 345.

337 Zie in dit kader Van der Sloot 2010, p. 107 e.v. Van der Sloot bespreekt de wederkerige overeenkomst waarbij de persoonsgegevens van de betrokkene als economisch goed worden verhandeld tegen een ander economisch goed, te weten een sociale netwerkdienst als bijvoorbeeld Facebook.

338 Deze vordering heeft de verantwoordelijke jegens de betrokkene indien laatstgenoemde tekortschiet in het nakomen van de privacyovereenkomst.

339 Er is voor deze focus gekozen vanwege het feit dat de verantwoordelijke, zoals zal blijken, meer verplichtingen heeft dan de betrokkene.

'reguliere' artikel 6:265 BW. Een aandachtspunt hierbij is dat artikel 6:265 BW ziet op de ontbinding van wederkerige overeenkomsten. Hiervoor is geconcludeerd dat in voorkomende gevallen een privacyovereenkomst een eenzijdige overeenkomst kan zijn. Een ontbinding op grond van artikel 6:265 BW lijkt daarmee op voorhand niet mogelijk te zijn. In artikel 6:261 lid 2 BW is echter bepaald dat de bepalingen omtrent wederkerige overeenkomsten overeenkomstig van toepassing zijn op andere rechtsbetrekkingen, op voorwaarde dat die strekken tot het wederzijds verrichten van prestaties. In geval de privacyovereenkomst als een eenzijdige overeenkomst moet worden aangemerkt, wordt aan de voorwaarde tot het wederzijds verrichten van prestaties niet voldaan; slechts de verantwoordelijke neemt plichten op zich. Het tweede lid van artikel 6:261 BW lijkt derhalve geen mogelijkheden te bieden voor het kunnen ontbinden van de eenzijdige privacyovereenkomst. Desondanks lijkt ontbinding van de eenzijdige privacyovereenkomst mogelijk te zijn op grond van een arrest van de Hoge Raad van 14 april 2000.[340] De Hoge Raad overwoog ten aanzien van de mogelijkheid tot ontbinding van een niet-wederkerige overeenkomst: "De aard van een overeenkomst als de onderhavige die ertoe strekt dat de opdrachtnemer een inspanningsverplichting op zich heeft genomen ten behoeve van de opdrachtgever een koopovereenkomst tot stand te brengen, brengt mee dat de opdrachtgever de mogelijkheid behoort te hebben om voor het geval de opdrachtnemer zich niet of onvoldoende van deze verplichting kwijt, op die grond de overeenkomst te beëindigen".

Uit artikel 6:267 BW wordt duidelijk dat de betrokkene de privacyovereenkomst kan ontbinden aan de hand van een langs elektronische weg uitgebrachte verklaring. Deze mogelijkheid is geïntroduceerd met de Aanpassingswet Richtlijn inzake Elektronische handel. Voordien was ontbinding slechts mogelijk via een schriftelijke verklaring of op vordering van de rechter. In ongewijzigde vorm van artikel 6:267 BW zou deze bepaling ertoe leiden dat ook in gevallen waarin de overeenkomst langs elektronische weg tot stand zou zijn gekomen de ontbinding daarvan steeds schriftelijk of door rechterlijke tussenkomst zou moeten geschieden. Een dergelijke situatie was voor de wetgever niet acceptabel, aldus de MvT van de Aanpassingswet.[341]

3.6.2 Ontbinding wegens het door de verantwoordelijke niet voldoen aan de informatieplicht voorafgaand aan en ten tijde van de totstandkoming van de privacyovereenkomst.

De verantwoordelijke heeft op grond van het BW een aantal informatieplichten dat hij jegens de betrokkene in acht heeft te nemen. De informatieplichten zijn bedoeld om de betrokkene meer duidelijkheid (transparantie) te bieden, waardoor het vertrouwen van de betrokkene in het elektronisch zaken doen wordt vergroot.[342] De Aanpassingswet richtlijn inzake

340 HR 14 april 2000 (*Van Ravenstein/Alves*), *NJ* 2000, 438; *RvdW* 2000, 106; *JOL* 2000, 225.

341 Kamerstukken II, 2001-2002, 28197, nr.3, p. 60 e.v.

342 Kamerstukken II 2001-2002, 28197, nr. 3, p. 55.

elektronische handel expliciteert dat bepaalde informatie voor de betrokkene van essentieel belang is op het moment dat hij op elektronische wijze een overeenkomst sluit. Het niet tijdig beschikken over deze informatie geeft de betrokkene het recht de overeenkomst te ontbinden.[343] Dit betekent dat, naast de reguliere mogelijkheid om een overeenkomst te ontbinden op grond van artikel 6:265 BW, het BW additionele mogelijkheden aan de wederpartij van de dienstverlener geeft om een overeenkomst te kunnen ontbinden. De vraag is of de betrokkene deze additionele (rechts)maatregelen kan inroepen indien de verantwoordelijke zijn verplichtingen die hij heeft uit hoofde van de privacyovereenkomst, niet naleeft. In het onderstaande wordt eerst bekeken welke mogelijkheden de betrokkene heeft om een overeenkomst ter zake het leveren van diensten of producten te kunnen ontbinden indien de verantwoordelijke zijn informatieplichten uit het BW niet nakomt. Vervolgens wordt onderzocht of deze ontbindingsmogelijkheid ook toepasbaar is op de privacyovereenkomst.

Artikel 6:227b BW legt aan de verantwoordelijke informatieplichten op die hij jegens de betrokkene op duidelijke, begrijpelijke en ondubbelzinnige wijze dient na te komen *voordat* een overeenkomst die ziet op het leveren van diensten of producten langs elektronische weg tot stand komt. Verzaakt de verantwoordelijke aan deze verplichtingen te voldoen, dan heeft de betrokkene de mogelijkheid om de tot stand gekomen overeenkomst te ontbinden zolang de verantwoordelijke hier niet aan heeft voldaan (artikel 6:227b lid 5 BW). Ten eerste dient de verantwoordelijke op grond van artikel 6:227b lid 1 onder b BW de betrokkene te informeren of hij de overeenkomst al dan niet archiveert en op welke wijze de overeenkomst, in geval van archivering, door de betrokkene te raadplegen is. Ten tweede zal de verantwoordelijke aan de betrokkene kenbaar moeten maken aan welke gedragscodes hij zich heeft onderworpen en de wijze waarop deze gedragscodes voor de betrokkene langs elektronische weg te raadplegen zijn, aldus artikel 6:227b lid 1 sub e BW. Tenslotte heeft de verantwoordelijke uit hoofde van artikel 6:227b lid 2 BW de verplichting om voor of bij het sluiten van de overeenkomst de voorwaarden daarvan, niet zijnde algemene voorwaarden als bedoeld in artikel 6:231 BW, op zodanige wijze aan de betrokkene ter beschikking te stellen, dat deze door hem kunnen worden opgeslagen zodat deze voor hem toegankelijk zijn ten behoeve van latere kennisneming. Ik wil er andermaal op wijzen dat artikel 6:227b BW van toepassing is indien er sprake is van elektronisch contracteren. Mocht een elektronisch uitgebracht aanbod uiteindelijk op schriftelijke wijze worden aanvaard, bijvoorbeeld door het plaatsen van een handtekening op een papieren document, dan hoeft de verantwoordelijke niet te voldoen aan de voorwaarden uit artikel 6:227b BW. Tevens wordt in het derde lid van dit artikel bepaald dat de verantwoordelijk de informatie zoals genoemd in artikel 6:227b lid 1 BW niet behoeft te verstrekken indien er sprake is van overeenkomst die uitsluitend door middel van de uitwisseling van

[343] De betrokkene heeft ook de mogelijkheid om de overeenkomst te vernietigen. Deze mogelijkheid wordt besproken in paragraaf 3.7.

elektronische post of soortgelijke vorm van individuele communicatie (bijvoorbeeld SMS) tot stand is gekomen.

De voornoemde informatieplichten zijn van toepassing op de overeenkomst die tussen de verantwoordelijke en de betrokkene langs elektronische weg tot stand is gekomen en die ziet op het leveren van diensten of producten. De privacyovereenkomst is geen dienst van de informatiemaatschappij, maar ziet wel op een dienst van de informatiemaatschappij. Vanwege deze samenhang kan mijns inziens worden betoogd dat de informatieplichten uit artikel 6:227b BW ook dienen te gelden voor de privacyovereenkomst.[344] Dit zou tot gevolg hebben dat de betrokkene de privacyovereenkomst kan ontbinden zolang de verantwoordelijke de informatie, zoals bedoeld in artikel 6:227b lid 1, onder b en e en lid 2 BW niet aan hem heeft verstrekt.

Behalve artikel 6:227b BW legt ook artikel 7:46c BW plichten aan de verantwoordelijke op die hij jegens de betrokkene dient na te komen voordat de overeenkomst wordt afgesloten. De bepalingen uit dit artikel zien specifiek op de koop op afstand.[345] Een nadere bestudering leert dat de opgenomen plichten met name product- dan wel dienstspecifiek van aard zijn. Dit heeft tot gevolg dat de betrokkene de privacyovereenkomst niet kan ontbinden op grond van dit artikel, althans niet direct kan ontbinden. In paragraaf 3.1 is gerefereerd aan de samenhang tussen de overeenkomst die ziet op het leveren van producten of diensten en de privacyovereenkomst. De privacyovereenkomst kan mijns inziens, als gevolg van de nauwe verbondenheid met de hoofdovereenkomst, door de betrokkene worden ontbonden indien hij tevens overgaat tot ontbinding van de hoofdovereenkomst op grond van artikel 7:46d lid 1 BW juncto artikel 7:46c BW.

3.6.3 Ontbinding op grond van het niet bevestigen van de aanvaarding van de betrokkene

Artikel 6:227c lid 2 BW regelt op welke wijze de verantwoordelijke dient te handelen na ontvangst van de op elektronische wijze gedane aanvaarding door de betrokkene van de privacyovereenkomst. Dit artikel biedt daarmee als het ware een ‘stappenplan’ dat in acht genomen dient te worden door de partij die op elektronische wijze een aanbod heeft gedaan. Voor de verantwoordelijke en de betrokkene luidt het stappenplan als volgt:

Stap 1: De verantwoordelijke doet langs elektronische weg een aanbod in de vorm van de privacyverklaring.

Stap 2: De betrokkene aanvaardt langs elektronische weg de privacyverklaring, waarmee de privacyovereenkomst tot stand komt.

Stap 3: De verantwoordelijke bevestigt zo spoedig mogelijk langs elektronische weg de ontvangst van de verklaring van aanvaarding aan de betrokkene.

---

344 Hetgeen geldt voor artikel 6:227b BW geldt mutatis mutandis ten aanzien van artikel 6:227c BW.

345 De definitie van ‘koop op afstand’ is bepaald in artikel 7:46a sub b BW.

Zolang de ontvangst van de aanvaarding niet door de verantwoordelijke aan de betrokkene is bevestigd, kan de betrokkene de privacyovereenkomst ontbinden op grond van artikel 6:227c lid 2 BW. Er zij op gewezen dat de privacyovereenkomst tussen de verantwoordelijke en de betrokkene tot stand is gekomen nadat de betrokkene heeft voldaan aan Stap 2 en deze verklaring van de betrokkene toegankelijk is geworden voor de verantwoordelijke.[346] Het niet voldoen aan Stap 3 geeft de betrokkene de mogelijkheid om de privacyovereenkomst aan te tasten door ontbinding. Het ontbinden van de privacyovereenkomst is niet meer mogelijk nadat de ontvangstbevestiging van de verantwoordelijke voor de betrokkene toegankelijk is geworden.[347]

3.6.4 Ontbinding ten gevolge van het intrekken ondubbelzinnige toestemming

In paragraaf 3.3 werd besproken dat een grondslag voor het mogen verwerken van persoonsgegevens is gelegen in het verstrekken van 'ondubbelzinnige toestemming' (artikel 8 sub a Wbp). Deze 'ondubbelzinnige toestemming' kan door de betrokkene worden gegeven met behulp van de privacyovereenkomst. Op grond van artikel 5 lid 2 Wbp heeft de betrokkene het recht om zijn verstrekte toestemming te allen tijde in te trekken. Indien de betrokkene van dit recht gebruik maakt, heeft dit tot gevolg dat verwerkingen die plaatsvinden op basis van ondubbelzinnige toestemming dienen te worden gestaakt.[348] Een intrekking van de toestemming lijkt weinig tot geen gevolgen te hebben voor de overeenkomst die ziet op de aanschaf van een product dan wel afname van een dienst. De verantwoordelijke zou zich immers op het standpunt kunnen stellen dat hij die gegevens mag blijven verwerken die noodzakelijk zijn voor de uitvoering van de overeenkomst, conform artikel 8 sub b Wbp. Uit de MvT wordt echter duidelijk dat een dergelijk verweer niet zal slagen. "Het is denkbaar dat de betrokkene zijn toestemming verleent om in het kader van de uitvoering van de overeenkomst of in een precontractuele fase gegevens van hem te verwerken. De gegevensverwerking steunt dan op artikel 8, onder a, indien althans de toestemming rechtsgeldig is verleend. De betrokkene heeft dan te allen tijde het recht zijn toestemming in te trekken, ten gevolge waarvan de rechtsgrondslag aan de gegevensverwerking komt te ontvallen. Het is dan de verantwoordelijke niet toegestaan alsnog op grond van artikel 8, onder b, tot verwerking over te gaan. Dit stuit op de norm van artikel 6: de verwerking geldt dan als onbehoorlijk en onzorgvuldig ten opzichte van de betrokkene".[349] Indien de verantwoordelijke als gevolg van het intrekken van de toestemming door de betrokkene de overeenkomst die ziet op de koop van een product of

346 Siemerink verwoordt het als volgt: "Ook zonder ontvangstbevestiging zijn beide partijen gebonden aan de overeenkomst, de ontvangstbevestiging kan daarom worden opgevat als een postcontractuele informatieplicht". Siemerink, p. 61.

347 Op grond van artikel 6:227c lid 3 BW.

348 Groep Gegevensbescherming Artikel 29-2011, p. 9. "The notion of control is also linked to the fact that the data subject should be able to withdraw his consent. Withdrawal is not retroactive, but it should, as a principle, prevent any further processing of the individual's data by the controller".

349 Kamerstukken II 1997-1998, 25892, nr. 3, p. 81 e.v.

dienst niet meer kan nakomen, zal dit een ontbinding van die overeenkomst tot gevolg hebben. Gezien de samenhang tussen die overeenkomst en de privacyovereenkomst, zal daarmee tevens de privacyverklaring kunnen worden ontbonden.[350]

3.7 Vernietiging en nietigheid van de privacyovereenkomst

In het navolgende wordt bezien op welke gronden de betrokkene de privacyovereenkomst mogelijk kan vernietigen, dan wel de nietigheid van de privacyovereenkomst kan inroepen. Paragraaf 3.7.1 analyseert of de betrokkene de privacyovereenkomst kan vernietigen indien de verantwoordelijke bepaalde informatieplichten uit het BW niet naleeft. De betrokkene kan mogelijk ook de privacyovereenkomst vernietigen indien er sprake is van dwaling. Deze grond van vernietiging wordt besproken in paragraaf 3.7.2. Tenslotte wordt in paragraaf 3.7.3 onderzocht of de betrokkene de nietigheid van de privacyverklaring kan inroepen indien er geen sprake is van ondubbelzinnige toestemming van de betrokkene.

3.7.1 Vernietiging wegens het door de verantwoordelijke niet voldoen aan de informatieplicht

In paragraaf 3.6.2. is gerefereerd aan artikel 6:227b BW. Hieruit volgde dat de verantwoordelijke bepaalde informatieplichten in acht dient te nemen jegens de betrokkene, en de betrokkene de overeenkomst kan ontbinden zolang de verantwoordelijke niet aan zijn informatieplicht heeft voldaan. Artikel 6:227b BW bevat, naast de reeds genoemde, nog enkele aanvullende informatieplichten voor de verantwoordelijke. Indien hij deze verplichting niet nakomt, heeft de betrokkene de mogelijkheid om de overeenkomst te vernietigen.

> Artikel 6:227b lid 1 aanhef, sub a, c, d en lid 4 BW
> 1. Voordat een overeenkomst langs elektronische weg tot stand komt verstrekt degene die een dienst van de informatiemaatschappij verleent als bedoeld in artikel 15d lid 3 van Boek 3 de wederpartij ten minste op duidelijke, begrijpelijke en ondubbelzinnige wijze informatie over:
> a. de wijze waarop de overeenkomst tot stand zal komen en in het bijzonder welke handelingen daarvoor nodig zijn;
> c. de wijze waarop de wederpartij van door hem niet gewilde handelingen op de hoogte kan geraken, alsmede de wijze waarop hij deze kan herstellen voordat de overeenkomst tot stand komt;

[350] Zie HR 23 januari 1998 (*Jans/FCN*), LJN: ZC2555, waaruit volgt dat samenhang tussen overeenkomsten dient te worden vastgesteld aan de hand van de uitleg van de rechtsverhouding tussen partijen in het licht van de omstandigheden. Zo ook HR 14 januari 2000 (*Meisnner/Arenda*), LJN: AA4279. Zie tevens HR 20 januari 2012 (*Agfaphoto/Foto Noort*), LJN: BU3162 met conclusie van Wuisman. In dit arrest werd samenhang aangenomen op basis van nauwe feitelijk-economische verbondenheid tussen twee overeenkomsten. Zie in dit kader tevens Van Laarhoven die factoren benoemt die betekenis hebben bij het vaststellen van rechtsplichten in samenhangende rechtsverhoudingen. Van Laarhoven, p. 90 e.v.

d. de talen waarin de overeenkomst kan worden gesloten;

4. Een overeenkomst die tot stand is gekomen onder invloed van het niet naleven door de dienstverlener van zijn in lid 1, aanhef en onder a, c of d, genoemde verplichtingen, is vernietigbaar. Indien de dienstverlener zijn in lid 1, aanhef en onder a of c genoemde verplichting niet is nagekomen, wordt vermoed dat een overeenkomst onder invloed daarvan tot stand is gekomen.

Aan de hand van de te verstrekken informatie moet het voor de betrokkene duidelijk worden op welke wijze een overeenkomst tot stand komt en welke handelingen daarvoor nodig zijn. Tevens moet het de betrokkene duidelijk zijn of hij bij de invoer van gegevens niet abusievelijk onjuiste gegevens heeft ingevoerd en op welke wijze hij vervolgens een foutieve invoer kan herstellen. Voorts is het van belang te weten in welke talen de overeenkomst kan worden gesloten.[351]

Op grond van artikel 6:227b lid 4 BW is een overeenkomst die tot stand is gekomen onder invloed van het niet naleven door de verantwoordelijke van zijn in artikel 6:227b lid 1 onder a, c, of d genoemde plichten, vernietigbaar. De MvT stelt dat de bedoelde informatie van essentieel belang is bij de wils- of oordeelsvorming van de wederpartij: “Indien de overeenkomst onder invloed van het niet verstrekt zijn van die informatie tot stand is gekomen, dient de wederpartij derhalve in staat te zijn zichzelf in de situatie te brengen die zou hebben bestaan indien in het geheel geen overeenkomst tot stand tot stand was gekomen”.[352]

Ter versterking van de bewijspositie van de wederpartij bepaalt artikel 6:227b lid 4 BW dat in geval de dienstverlener zijn in artikel 6:227b lid 1, aanhef en onder a of c BW genoemde verplichting niet is nagekomen, wordt vermoed dat de overeenkomst onder invloed daarvan tot stand is gekomen. De MvT rechtvaardigt dit door te stellen dat de bedoelde informatie naar haar aard steeds rechtstreeks van invloed is op de vraag of een overeenkomst tot stand komt en of deze overeenkomst de door de wederpartij bedoelde inhoud heeft. Daarbij is het derhalve redelijk te veronderstellen dat het ontbreken van die informatie invloed heeft gehad op de wilsvorming van de wederpartij.[353]

Waar artikel 6:227b BW lid 1 sub c BW ziet op de plicht van de dienstverlener om de wederpartij te informeren over de wijze waarop hij van door hem niet gewilde handelingen op de hoogte kan geraken, alsmede de wijze waarop hij deze kan herstellen voordat de

---

351 In de MvT van de Aanpassingswet wordt erop gewezen dat de “de informatieplichten beogen te voorkomen dat de wederpartij onbewust of onbedoeld een overeenkomst sluit of, omgekeerd, meent een overeenkomst te hebben gesloten terwijl daarvoor nog meer handelingen zijn vereist”. Kamerstukken II, 2002/2003, 28197, nr.3, p. 55 e.v.

352 Kamerstukken II, 2001-2002, 28197, nr.3, p. 56.

353 Kamerstukken II, 2001-2002, 28197, nr.3, p. 56.

overeenkomst tot stand komt, heeft artikel 6:227c lid BW lid 1 BW betrekking op de plicht van de dienstverlener om passende, doeltreffende en toegankelijke middelen aan de wederpartij ter beschikking te stellen. Dit dient hij op een zodanige wijze te doen dat de wederpartij voor aanvaarding van de overeenkomst op de hoogte kan geraken van door hem niet gewilde handelingen en de herstelmogelijkheden. De MvT wijst er overigens op dat deze bepaling mede in het belang is van de aanbieder zelf, aangezien deze hierdoor meer zekerheid krijgt dat de aldus tot stand gekomen overeenkomsten ook daadwerkelijk rechtsgeldig tot stand komen en in principe onaantastbaar zijn.[354] Indien de verantwoordelijke zijn plicht uit hoofde van artikel 6:227b lid 1 BW niet nakomt, kan de betrokkene de overeenkomst vernietigen. Artikel 6:227c lid 5 BW bepaalt dat in geval de verantwoordelijke zijn in lid 1 genoemde verplichting niet is nagekomen, wordt vermoed dat de overeenkomst onder invloed daarvan tot stand is gekomen.

3.7.2 Vernietiging van de privacyovereenkomst op grond van dwaling

Dwaling, ofwel de afwezigheid van een juiste voorstelling van zaken, is een grond voor vernietiging van een overeenkomst. De vereisten waaraan in ieder geval moet zijn voldaan wil er sprake zijn van dwaling zijn neergelegd in artikel 6:228 lid 1 BW.

> Artikel 6:228 BW
> 1. Een overeenkomst die is tot stand gekomen onder invloed van dwaling en bij een juiste voorstelling van zaken niet zou zijn gesloten, is vernietigbaar:
> a. indien de dwaling te wijten is aan een inlichting van de wederpartij, tenzij deze mocht aannemen dat de overeenkomst ook zonder deze inlichting zou worden gesloten;
> b. indien de wederpartij in verband met hetgeen zij omtrent de dwaling wist of behoorde te weten, de dwalende had behoren in te lichten;
> c. indien de wederpartij bij het sluiten van de overeenkomst van dezelfde onjuiste veronderstelling als de dwalende is uitgegaan, tenzij zij ook bij een juiste voorstelling van zaken niet had behoeven te begrijpen dat de dwalende daardoor van het sluiten van de overeenkomst zou worden afgehouden.
> 2. De vernietiging kan niet worden gegrond op een dwaling die een uitsluitend toekomstige omstandigheid betreft of die in verband met de aard van de overeenkomst, de in het verkeer geldende opvattingen of de omstandigheden van het geval voor rekening van de dwalende behoort te blijven.

Dwaling kan worden onderscheiden in eigenlijke en oneigenlijke dwaling. Er is sprake van dwaling in eigenlijke zin indien er tussen de verantwoordelijke en de betrokkene wilsovereenstemming bestaat, doch de wil van een der partijen zich heeft gevormd onder invloed van een valse voorstelling. Oneigenlijke dwaling houdt in dat er geen

[354] Kamerstukken II, 2001-2002, 28197, nr.3, p. 58.

wilsovereenstemming tot stand is gekomen als gevolg van een vergissing of een misverstand.[355] Het is niet ondenkbaar dat de betrokkene, op grond van het hebben gezien van de inhoud van de privacyovereenkomst, ervan uit is gegaan dat de verantwoordelijke de persoonsgegevens op behoorlijke en zorgvuldige wijze zal verwerken. Indien achteraf zou blijken dat de betrokkene zich hierin heeft vergist, kan hij de privacyovereenkomst mogelijk vernietigen met een beroep op dwaling. Dit is echter niet mogelijk indien de dwaling voor rekening van de betrokkene komt.[356] Of dit laatste daadwerkelijk het geval is, is afhankelijk van de in het verkeer geldende opvattingen of de aard van de overeenkomst. Het is verdedigbaar dat de betrokkene de privacyovereenkomst *niet* kan vernietigen op grond van dwaling indien de verantwoordelijke de betrokkene vooraf heeft gewezen op het bestaan van de privacyovereenkomst en de betrokkene door de privacyovereenkomst heeft laten 'scrollen' alvorens hij deze kon aanvaarden. Anderzijds is in paragraaf 3.5 de vraag opgeworpen of de betrokkene überhaupt de inhoud van een privacyverklaring kan begrijpen. Of de betrokkene een geslaagd beroep op dwaling kan doen, is mede afhankelijk van de mate van transparantie die met betrekking tot de inhoud van de privacyovereenkomst wordt betracht.

3.7.3 Vernietiging op grond van artikel 6:248 BW

Tot slot zou de betrokkene, mocht bijvoorbeeld een beroep op dwaling zoals besproken in de vorige paragraaf niet slagen, mogelijk de privacyovereenkomst - al dan niet geheel of gedeeltelijk - kunnen vernietigen door een beroep te doen op artikel 6:248 lid 2 BW. Op grond van deze bepaling kan een tussen de verantwoordelijke en de betrokkene geldende afspraak niet van toepassing worden verklaard indien deze in een gegeven omstandigheid naar maatstaven van redelijkheid en billijkheid onaanvaardbaar zou zijn.[357] Anderzijds zou de betrokkene mogelijk een beroep kunnen doen op lid 1 van artikel 6:248 BW. In dit lid is bepaald dat een overeenkomst niet alleen de door partijen overeengekomen rechtsgevolgen heeft, maar ook die bijvoorbeeld voortvloeien uit gewoonte. Het is voorstelbaar dat de privacyovereenkomst in sterke mate afwijkt van een privacyverklaring (of privacyovereenkomst) die gebruikelijk binnen een bepaalde branche wordt gehanteerd. In dat geval zou de betrokkene zich op het standpunt kunnen stellen dat de bestaande privacyovereenkomst - al dan niet geheel of gedeeltelijk - dient te worden vernietigd, en dat vervolgens de in die branche gehanteerde privacyverklaring van toepassing wordt verklaard op de rechtsverhouding tussen de verantwoordelijke en de betrokkene.[358]

---

355 Zie ook Asser/Hartkamp/Sieburgh, nr. 218.

356 Op grond van artikel 6:228 lid 2 BW.

357 Zie in dit kader Siemerink et al., p. 148.

358 Anderzijds zou de betrokkene naleving van de privacyovereenkomst kunnen vorderen, waarbij de rechtsverhouding tussen hem en de verantwoordelijke, op grond van artikel 6:248 lid 1 BW, nader wordt ingekleurd aan de hand van een binnen die branche gebruikelijke privacyverklaring (overeenkomst). Evenzo is het denkbaar dat op grond van artikel 6:248 lid 1 BW een binnen een branche gebruikelijke privacyverklaring van toepassing wordt verklaard op de rechtsverhouding

3.7.4 Nietigheid wegens het ontbreken van ondubbelzinnige toestemming.

Conform artikel 8 sub a Wbp is een verwerking van persoonsgegevens toegestaan indien de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven. Eerder is opgemerkt dat deze toestemming kan worden geven aan de hand van de privacyovereenkomst.[359] Tevens kwam aan de orde dat de MvT stelt dat een rechtshandeling die door inhoud of strekking in strijd is met de goede zeden of de openbare orde nietig is op grond van artikel 3:40 lid 1 BW. In dat kader expliciteert de MvT dat toestemming die met betrekking tot een bepaalde gegevensverwerking niet rechtsgeldig is gegeven, als nietig moet worden beschouwd.[360] Dit heeft tot gevolg dat de privacyovereenkomst deels nietig is, indien de feitelijke handelingen, die door de betrokkene bij de aanvaarding van de privacyovereenkomst zijn verricht, niet dusdanig waren dat van ondubbelzinnige toestemming gesproken kan worden. Het ontbreken van ondubbelzinnige toestemming heeft niet tot gevolg dat de gehele privacyovereenkomst nietig is. De nietigheid raakt de afspraken in de privacyovereenkomst die zien op verwerkingen waarvoor, op grond van artikel 8 sub a Wbp, een ondubbelzinnige toestemming vereist is.

3.8 Schadevergoeding

Indien de verantwoordelijke tekortschiet in de nakoming van de privacyovereenkomst, is hij op grond van artikel 6:74 BW gehouden de schade te vergoeden die de betrokkene als gevolg daarvan zal lijden. De betrokkene heeft op grond van artikel 6:95 BW de mogelijkheid om vermogensschade te vorderen, alsmede schadevergoeding voor geleden nadeel dat niet uit vermogensschade bestaat.[361]

Artikel 6:106 BW bepaalt ten aanzien van nadeel dat niet uit vermogensschade bestaat, dat de betrokkene recht heeft op een naar billijkheid vast te stellen schadevergoeding. Men spreekt van een ‘ander nadeel’ voor zover het gaat om resterend nadeel dat niet eenvoudig tot het vermogen is te herleiden.[362] Volgens Verburg lijkt een vermindering van welzijn vooralsnog de meest treffende en feitelijke omschrijving van het begrip ‘ander nadeel dan vermogensschade’.[363] Het eerste lid van artikel 6:106 BW noemt limitatief de gevallen die grond geven voor een vergoeding wegens geleden immateriële schade. Bij sub b gaat het daarbij over persoonsaantastingen, onderverdeeld in lichamelijk letsel, schending van eer

---

tussen de verantwoordelijke en de betrokkene indien de verantwoordelijke überhaupt geen privacyverklaring op zijn website heeft geplaatst. Zie in dit kader tevens paragraaf 6.3.5.

359 In paragraaf 3.5 is een voorbeeld gegeven van de feitelijke handelingen die de betrokkene moeten verrichten wil er sprake zijn ondubbelzinnige toestemming.

360 Kamerstukken II 1997-1998, 25892, nr. 3, p. 67.

361 Zie artikel 6:96 BW en artikel 6:106 BW.

362 Lindenbergh, p. 21.

363 Verburg, p. 34.

en goede naam en aantasting van de persoon op een andere wijze.[364] Lindenbergh betoogt dat 'persoonsaantasting op een andere wijze' nader kan worden vormgegeven door een onderscheid te maken tussen geestelijk letsel en schending van persoonlijkheidsrechten.[365] Met betrekking tot laatstgenoemd onderscheid heeft de Hoge Raad overwogen dat schending van bepaalde fundamentele rechten als zodanig een recht op smartengeld kan rechtvaardigen, ook zonder dat sprake is van lichamelijk of geestelijk letsel.[366] Relevant is hier het arrest *Groninger Oudejaarsrellen*, waarin de Hoge Raad aanvaardt dat het uitblijven van een reactie van de politie tijdens rellen waarin een woning werd belegerd een zeer ernstige inbreuk op de integriteit van de persoon en de veiligheid van de woning en zijn bewoners vormt.[367] Op grond van schending van deze fundamentele rechten kende de Hoge Raad smartengeld toe. Eveneens van belang is het arrest *Baby Kelly*.[368] Deze zaak betrof een verloskundige die had nagelaten om prenatale diagnostiek aan te bieden, waardoor niet tijdig kon worden ontdekt dat de foetus een chromosomale afwijking had. De Hoge Raad overwoog dat "Wanneer aan de moeder de uitoefening van haar keuzerecht wordt onthouden door een fout van een verloskundige en zij daarmee, zoals in de onderhavige zaak, niet ervoor heeft kunnen kiezen de geboorte van een zwaar gehandicapt kind te voorkomen, een ernstige inbreuk wordt gemaakt op haar zelfbeschikkingsrecht..." en "Een zo ingrijpende aantasting als in dit geding aan de orde van een zo fundamenteel recht moet worden aangemerkt als een aantasting in de persoon in de zin van art. 6:106 lid 1, aanhef en onder b, BW, zonder dat nodig is dat geestelijk letsel is vastgesteld".[369] Verburg tekent aan dat er nog geen catalogus bestaat van beschermingswaardige fundamentele rechten, maar verduidelijkt dat bijvoorbeeld schending van de persoonlijke levenssfeer (privacy) valt onder de noemer schending van een persoonlijkheidsrecht.[370]

3.9 De privacyverklaring als elektronische algemene privacyvoorwaarden

De privacyverklaring die op de website van de verantwoordelijke via een hyperlink wordt weergegeven, veelal *naast* algemene voorwaarden, kan mogelijk *ook* worden gekwalificeerd als algemene voorwaarden.[371] Siemerink stelt dat, behoudens kernbedingen, alle andere

364 Lindenbergh, p. 24.
365 Lindenbergh, p. 31 e.v.
366 Lindenbergh, p. 34.
367 HR 9 juli 2004 (*Groninger Oudejaarsrellen*), NJ 2005, 391 m.nt. J.B.M. Vranken.
368 HR 18 maart 2005 (*Baby Kelly*), NJ 2006, 606 m.nt. J.B.M. Vranken.
369 HR 18 maart 2005, r.o. 4.8.
370 Verburg verwijst hierbij naar het arrest *Groninger Oudejaarsrellen*. Verburg, p 161.
371 Ook in een disclaimer kunnen bepalingen omtrent de verwerking van persoonsgegevens worden opgenomen (zoals zal blijken in hoofdstuk 4). Zie in dit kader Siemerink et al, die stellen dat in het geval een disclaimer deel uit maakt van een overeenkomst, deze zou kunnen worden aangemerkt als algemene voorwaarden. Siemerink et al., p. 145.

online voorwaarden per definitie algemene voorwaarden zijn.[372] Indien we de argumentatie van Siemerink volgen, betekent dit dat de privacyverklaring als 'algemene privacyvoorwaarden' kan worden gekwalificeerd.[373] Dit zal mede tot gevolg hebben dat de betrokkene, indien hij de gelding van de algemene privacyvoorwaarden aanvaardt, gebonden zal zijn aan die algemene privacyvoorwaarden, zelfs als hij bij het sluiten van de overeenkomst de inhoud van de algemene privacyvoorwaarden niet kent.[374] In deze paragraaf zal dit nader worden onderzocht, waarbij wordt aangetekend dat 'slechts' een aantal essentiële kenmerken van algemene voorwaarden wordt benoemd. Deze zullen vervolgens in de context van de privacyverklaring worden geplaatst.[375]

De verhouding tussen algemene voorwaarden en de verwerking van persoonsgegevens is een terugkerend punt van aandacht in de literatuur. Thijssen stelt in het kader van de informatieplicht die volgt uit de artikelen 33 en 34 Wbp dat het voldoende is om de informatie op te nemen in een privacystatement of in algemene voorwaarden ter voldoening aan de informatieplicht.[376] Cuijpers is van mening dat een beding in algemene voorwaarden op grond waarvan de betrokkene verklaart akkoord te zijn met de verwerking van de hem betreffende persoonsgegevens, gezien de strenge vereisten die zowel de Privacyrichtlijn als het algemene privaatrecht stelt met het verlenen van toestemming, in strijd is met het recht.[377] Rodrigues betoogt dat toestemming onder omstandigheden wel impliciet kan worden verstrekt, maar dat daarvan bij een gefingeerde wilsverklaring in de algemene voorwaarden geen sprake van is.[378] Berkvens meent dat bedrijven aan de hand van algemene voorwaarden consumenten kunnen informeren over de wijze waarop wordt omgegaan met persoonsgegevens. "Standard terms and conditions can be used to explain the policy of enterprises on the use of customers' personal data".[379] Het voordeel van het gebruik van algemene voorwaarden als informatie-instrument is, aldus Berkvens, gelegen in het feit dat algemene voorwaarden dicht bij de dagelijkse praktijk staan. "Standard terms and conditions are close to the day-to-day reality and regulate specific situations".[380]

Algemene voorwaarden worden in artikel 6:231 BW omschreven als een of meer bedingen die zijn opgesteld teneinde in een aantal overeenkomsten te worden opgenomen, met

372 Siemerink, p. 58.
373 Ter voorkoming van onduidelijkheid wordt in deze paragraaf de term algemene privacyvoorwaarden gehanteerd.
374 Asser/Hartkamp/Sieburgh 6III, p. 401.
375 Voor een uitgebreide verhandeling over algemene voorwaarden zie Wessels, Jongeneel & Hendrikse, Asser/Hartkamp/Sieburgh en Van Wechem.
376 Thijssen, p. 236.
377 Cuijpers 2004, p. 173.
378 Rodrigues, p. 46.
379 Berkvens 2009-a, p. 129.
380 Berkvens 2009-a, p. 129.

uitzondering van bedingen die de kern van de prestaties aangeven. Er dient aan drie vereisten te zijn voldaan wil sprake zijn van algemene voorwaarden:

1. Er moet sprake zijn van één of meer bedingen. Onder bedingen wordt verstaan voorwaarden van contractuele aard[381];
2. Deze bedingen dienen te zijn opgesteld teneinde in een aantal overeenkomsten te worden opgenomen; en
3. Het mogen geen bedingen zijn die de kern van de prestaties aangeven. Als kernbedingen moeten worden aangemerkt de zogeheten essentialia van een overeenkomst. Dit zijn bestanddelen zonder welke de overeenkomst bij gebreke van voldoende bepaalbaarheid van de verbintenissen niet tot stand komt.[382]

In het geval er tussen de verantwoordelijke en de betrokkene een overeenkomst tot stand komt die ziet op de aanschaf van een product of de afname van een dienst, zullen de persoonsgegevens met name worden verwerkt ter uitvoering van die overeenkomst. Dientengevolge zijn de kernbedingen opgenomen in de hoofdovereenkomst, en niet in de privacyverklaring. Daarmee wordt voldaan aan de vereisten van artikel 6:231 BW, aangezien de privacyverklaring in dat geval bestaat uit een aantal bedingen, zijnde geen kernbedingen, die zijn opgesteld om in een aantal overeenkomsten te worden opgenomen.

Het staat de verantwoordelijke en de betrokkene geheel vrij om in een overeenkomst die ziet op de koop van een product of dienst te bepalen dat de algemene privacyvoorwaarden van toepassing zijn.[383] Een dergelijk bepaling is bindend indien de betrokkene de hoofdovereenkomst aanvaardt.[384] Artikel 6:232 BW bepaalt dat een wederpartij ook dan aan algemene voorwaarden is gebonden als bij het sluiten van de overeenkomst de gebruiker begreep of moest begrijpen dat hij de inhoud daarvan niet kende. Dit betekent dat de betrokkene gebonden is aan algemene voorwaarden, ook al is hij niet van de inhoud op de hoogte.[385] Maritius expliciteert derhalve dat, ingeval een overeenkomst langs elektronische

---

381 Jongeneel, p. 83.

382 Voor een inhoudelijke bespreking van het begrip kernbedingen wordt verwezen naar Jongeneel, p. 90 e.v.

383 Maritius benadrukt dat het van belang is dat het gebruik van de algemene voorwaarden duidelijk is tijdens het totstandkomingsproces van de overeenkomst in de zin dat de algemene voorwaarden onderdeel zijn van het aanbod van de gebruiker. Maritius, p. 383.

384 Vergelijk in deze Registratiekamer, p. 43. Hierin wordt gesteld als volgt: “Het is de vraag in hoeverre de abonnee toestemming geeft bij het aanvaarden van een kernbeding van de overeenkomst tussen de provider en de abonnee. In die situatie is er sprake van een wilsovereenstemming tussen partijen. De door de abonnee geuite wil kan als ondubbelzinnige toestemming worden gekwalificeerd voor zover daarbij voldaan is aan de vereisten die artikel 8, onder a van de Wbp hieraan stelt. In dat geval is de toestemming van de abonnee de grondslag voor de beoogde verwerking.”

385 Zo ook Loos: “Uit artikel 6:232 BW vloeit voort dat voor aanvaarding van de gelding niet is vereist dat de wederpartij kennis heeft genomen van de inhoud van de algemene voorwaarden of zelfs maar kennis van die inhoud heeft kunnen nemen. Voor ‘aanvaarding’ in de zin van artikel 6:231

weg tot stand komt, het voldoende is dat duidelijk naar het complex van algemene voorwaarden wordt verwezen.[386] De snelle gebondenheid van de betrokkene aan algemene voorwaarden blijkt tevens uit de antwoorden van de ministers van Justitie en van Economische Zaken naar aanleiding van vragen uit de Eerste Kamer over elektronische algemene voorwaarden. In antwoord op de vraag of kan worden volstaan met het opnemen van een algemene voorwaarden-(hyperlink) button op de website, of dat de wederpartij uitdrukkelijk langs de algemene voorwaarden moet worden geleid en zich uitdrukkelijk met de toepasselijkheid daarvan akkoord moet verklaren, antwoordden de ministers dat voor gebondenheid aan algemene voorwaarden nodig is dat de wederpartij akkoord is gegaan met de algemene voorwaarden als geheel. Daarbij wijzen ze erop dat er zelfs sprake kan zijn van gebondenheid indien de gebruiker begreep of moest begrijpen dat de wederpartij de inhoud van de voorwaarden niet kende. De ministers stellen tevens dat ten opzichte van de algemene regel tot snelle gebondenheid, de mogelijkheid voor de wederpartij bestaat om een beding in algemene voorwaarden te vernietigen indien het beding onredelijk bezwarend is dan wel indien de gebruiker de wederpartij geen redelijke mogelijkheid heeft geboden om van de algemene voorwaarden kennis te nemen. Het lijkt hen in dat verband voldoende indien duidelijk wordt aangegeven dat de algemene voorwaarden deel uitmaken van de overeenkomst en dat deze voorwaarden achter een duidelijk herkenbare hyperlink zijn opgenomen.[387] Dit standpunt lijkt te worden bevestigd op grond van artikel 6:234 lid 1 BW jo. artikel 6:230c lid 3 BW. Voorwaarde is daarbij wel dat dit op een zodanige wijze gebeurt dat de algemene voorwaarden door hem kunnen worden opgeslagen en voor hem toegankelijk zijn ten behoeve van latere kennisneming, aldus de ministers.[388] Met betrekking tot dit laatste wordt gedoeld op artikel 6:234 lid 2 BW. Uit dit artikel volgt onder meer dat de gebruiker aan de wederpartij een redelijke mogelijkheid heeft geboden om van de algemene voorwaarden kennis te nemen indien hij voor of bij het sluiten van de overeenkomst de algemene voorwaarden langs elektronische weg ter beschikking heeft gesteld op een zodanige wijze dat deze door hem kunnen worden opgeslagen en voor hem toegankelijk zijn ten behoeve van latere kennisneming.

In het licht van het voorgaande luidt de conclusie dat de betrokkene gebonden is aan de algemene privacyvoorwaarden zonder dat hij kennis heeft genomen van de inhoud, maar wel de toepasselijkheid van die algemene privacyvoorwaarden in de hoofdovereenkomst heeft aanvaard. De vraag is vervolgens of dit als bezwaarlijk dient te worden beschouwd.

---

sub c BW is derhalve voldoende dat de wederpartij weet dat de algemene voorwaarden deel uitmaken van de overeenkomst, en dat zij desalniettemin tot contractsluiting overgaat." Loos, p. 16.

386 Maritius, p. 383.

387 Kamerstukken I 2003-2004, 28197, C, p. 18.

388 Kamerstukken I 2003-2004, 28197, C, p. 18.

Het antwoord is mijns inziens ontkennend. Naar verwachting kent de algemene privacyverklaring meer verplichtingen voor de verantwoordelijke dan voor de betrokkene.[389] Mocht de inhoud van de algemene privacyvoorwaarden nadelig zijn voor de betrokkene, dan heeft hij diverse mogelijkheden om van die inhoud, al dan niet gedeeltelijk, bevrijd te worden. Ten eerste mag de inhoud van de privacyverklaring, op straffe van nietigheid, niet in strijd zijn met de Wbp. Ten tweede kan de betrokkene zich succesvol beroepen op de stelling dat ten aanzien van verwerkingen waarvoor ondubbelzinnige toestemming een vereiste is, deze toestemming ontbreekt. De betrokkene heeft immers bij de aanvaarding van de hoofdovereenkomst geen kennis genomen van de inhoud van de algemene privacyverklaring. Er kan vanuit het oogpunt van de Wbp slechts dan sprake zijn van rechtsgeldig gegeven toestemming indien deze op geïnformeerde basis heeft plaatsgevonden (het zogeheten informed consent). Het moet de betrokkene voordat hij zijn toestemming verstrekt duidelijk zijn welke verwerking het betreft, welke gegevens worden verwerkt en voor welk doel die verwerking zal plaatsvinden. Bovendien dient hij door verantwoordelijke geïnformeerd te zijn over alle overige aspecten van de gegevensverwerking die voor hem van belang zijn.[390] Van Esch en Blok stellen in dit verband dat kenmerkend voor algemene voorwaarden is dat deze als geheel kunnen worden aanvaard zonder dat de betrokkene kennis hoeft te nemen van de afzonderlijke bepalingen. “Derhalve kan zelfs bij expliciete aanvaarding van de voorwaarden de discussie ontstaan over de vraag of er expliciet toestemming is gegeven voor de in de voorwaarden omschreven gegevensverwerkingen”.[391] Ten derde kan de betrokkene, om bevrijd te worden van de gebondenheid aan bepalingen uit de algemene privacyvoorwaarden, zich op het standpunt stellen dat die bepalingen onredelijk bezwarend zijn conform artikel 6:233 sub a BW. Ten vierde kan de betrokkene een beding uit de algemene privacyvoorwaarden vernietigen indien deze voorwaarden door de verantwoordelijke op een zodanige wijze ter beschikking zijn gesteld dat de betrokkene de algemene privacyvoorwaarden niet kon opslaan.[392] Tot slot zou de betrokkene een voor hem nadelig beding kunnen vernietigen op grond van artikel 6:248 lid 2 BW.[393]

---

389 Dit is in afwijking van ‘reguliere algemene voorwaarden’ waarin veelal verplichtingen voor de wederpartij worden opgenomen, en waarin de verplichtingen van de gebruiker van die voorwaarden zoveel mogelijk worden beperkt.

390 Zie de in paragraaf 2.2.2.1 benoemde voorwaarden met betrekking tot ondubbelzinnige toestemming.

391 Van Esch & Blok, p. 213.

392 In hoofdstuk 4 (empirisch onderzoek) zal blijken dat in 91% van alle onderzochte privacyverklaringen de betrokkene niet de mogelijkheid heeft om de privacyverklaring te kunnen opslaan.

393 Zie in dit kader paragraaf 3.7.3.

3.10 Conclusie

In dit hoofdstuk stond de privacyverklaring vanuit het perspectief van het BW centraal, en in het bijzonder het overeenkomstenrecht. Geconcludeerd kan worden dat aan de hand van een privacyverklaring de verantwoordelijke een aanbod doet aan de betrokkene over de wijze waarop hij persoonsgegevens wil gaan verwerken. Mocht de betrokkene het aanbod van de verantwoordelijke aanvaarden dan resulteert dit in een privacyovereenkomst. De inhoud van de privacyovereenkomst wordt begrensd door de Wbp. Dit betekent dat de afspraken die de verantwoordelijke en de betrokkene in de privacyovereenkomst vastleggen niet in strijd mogen zijn met de Wbp. De privacyovereenkomst kan als instrument worden gebruikt bij het concretiseren van de informatieplicht die volgt uit de artikelen 33 en 34 Wbp. De verantwoordelijke kan in dat geval verplichtingen op zich nemen die verder gaan dan de verplichtingen die voor hem voortvloeien uit de Wbp. Het staat de verantwoordelijke en de betrokkene echter vrij om afspraken in de privacyovereenkomst op te nemen die niet noodzakelijkerwijs op grond van de Wbp behoeven te worden opgenomen.

We kunnen een aantal voor- en nadelen benoemen waar het gaat om het hanteren van het instrument van de overeenkomst ter concretisering van de informatieplicht (artikelen 33 en 34 Wbp). Beginnend bij de voordelen, kan als eerste worden gewezen op de mogelijkheid tot een nadere concretisering van de open normen uit de artikelen 33 en 34 Wbp. Aan de hand van de privacyovereenkomst maken de verantwoordelijke en de betrokkene concreet duidelijk onder welke omstandigheden zij van mening zijn dat sprake is van een voldoende informatieverstrekking opdat een behoorlijke en zorgvuldige verwerking van persoonsgegevens kan plaatsvinden. Het gevolg van deze concretisering is dat de juridische positie van de betrokkene sterker wordt, aangezien de privacyovereenkomst verduidelijkt wat de verantwoordelijke zal doen of nalaten. Een tweede voordeel is mogelijk gelegen in het versterken van de bewustwording van de verantwoordelijke en de betrokkene met betrekking tot de verwerking van persoonsgegevens. Met andere woorden, het afsluiten van een ‘overeenkomst’ draagt bij aan bewustwording. Het is immers niet ondenkbaar dat de verantwoordelijke zich bij het opstellen en het aangaan van een privacyovereenkomst beter realiseert dat hij verplichtingen heeft jegens de betrokkene ten aanzien van het verwerken van persoonsgegevens, maar ook welke verplichtingen hij heel concreet op zich neemt. Ook de betrokkene wordt zich er meer van bewust dat zijn persoonsgegevens worden verwerkt, en welke gegevens het betreft.
Er kleven ook nadelen aan het gebruik van een privacyovereenkomst. Ten eerste blijft onzekerheid bestaan of de overeengekomen inhoud voldoende conform de vereisten van artikelen 33 en 34 Wbp is. Bovendien zal de betrokkene in de dagelijkse praktijk geen invloed hebben, en daarmee niet betrokken worden bij het opstellen van de privacyovereenkomst. Naar verwachting zal hij ook niet in staat worden gesteld de inhoud van de privacyovereenkomst te wijzigen. Daarnaast is het absoluut niet ondenkbaar dat de

betrokkene, indien hij de inhoud van de privacyovereenkomst afwijst, überhaupt niet in staat wordt gesteld een product via de website aan te kopen. Daarbij: hoe weet de betrokkene dat er wel of niet in strijd met de privacyovereenkomst wordt gehandeld? En al heeft de betrokkene, op grond van het BW, de beschikking over een aantal rechtsmiddelen, het blijft voor hem complex die rechtsmaatregelen te overzien en toe te passen. Ook de verantwoordelijke kan bedenkingen hebben bij het gebruik van een privacyovereenkomst. Er blijft immers onzekerheid bestaan of de aanvaarding van de privacyovereenkomst door de betrokkene wel rechtsgeldig heeft plaatsgevonden. De betrokkene kan wel verklaren dat hij de privacyovereenkomst heeft gelezen en begrepen, maar is dat daadwerkelijk het geval? De verantwoordelijke neemt op grond van de privacyovereenkomst verplichtingen op zich. Echter, hoe meer verplichtingen hij op zich neemt, des te groter de kans is dat hij tekortschiet jegens de betrokkene. Ofwel, de kans is niet gering dat de verantwoordelijke de informatieverstrekking in de privacyovereenkomst zo beperkt mogelijk zal houden en zichzelf zo min mogelijk verplichtingen op zal leggen. In het navolgende hoofdstuk zullen we via een nadere empirische analyse van websites bezien of dit inderdaad het geval is.

In het licht van het voorgaande luidt de conclusie dat het instrument van de overeenkomst valt te hanteren ter concretisering van de informatieplicht uit de artikelen 33 en 34 Wbp. Het blijft echter een toepassing op ‘individueel’ niveau. Dat wil zeggen dat alleen de verantwoordelijke en de betrokkene als partijen betrokken zijn bij de totstandkoming en uitvoering van de privacyovereenkomst. Dit resulteert mogelijk in rechtsongelijkheid en rechtsonzekerheid. In hoofdstuk 6 zal worden onderzocht of de betrokkenheid van belangenorganisaties die rechtsongelijkheid en rechtsonzekerheid mogelijk kan inperken.

Hoofdstuk 4 | Empirisch onderzoek onder online winkels

4.1 Inleiding

In dit hoofdstuk wordt verslag gedaan van een onderzoek onder 257 online winkels in de marktsegmenten Verzekeringen, Reizen en Kleding. Het doel van het onderzoek is nader inzicht te krijgen in het feitelijk gebruik van de privacyverklaring in enkele sectoren. In paragraaf 4.2 e.v. wordt de opzet van het empirisch onderzoek besproken en verantwoording afgelegd over de wijze waarop het empirisch onderzoek is uitgevoerd. Paragraaf 4.7 e.v. presenteert de resultaten van het empirisch onderzoek, waarna dit hoofdstuk in paragraaf 4.13 wordt afgesloten met een systematische samenvatting en conclusies.

4.2 De keuze voor de online segmenten Verzekeringen, Reizen en Kleding

Sinds 1998 brengt het onderzoeksbureau BlauwResearch, in opdracht van de belangenvereniging Thuiswinkel.org, ieder half jaar de markt voor verkopen op afstand in kaart. Het doel van het onderzoek van BlauwResearch is “inzicht te krijgen in de markt voor bestedingen via thuiswinkel kanalen en specifiek het internet kanaal”, waarbij deze doelstelling zich laat vertalen naar “het leveren van periodieke informatie over de totale online thuiswinkel markt, specifieke segmenten voor online consumentenbestedingen en informatie over de Nederlandse online koper”.[394] De uitkomsten van het onderzoek worden door BlauwResearch gepresenteerd in de Thuiswinkel Markt Monitor, waarbij de navolgende online marktsegmenten worden onderscheiden:[395]

Online marktsegment	
Computer Hardware	Witgoed en Huishoudelijke- / keukenapparatuur
Consumenten Elektronica	Interieur- en tuinartikelen
Telecom	Tickets
Computer Software	Verzekeringsproducten
Home-entertainment	Levensmiddelen & persoonlijke verzorging
Boek / tijdschrift / krant	Sportartikelen
Muziek	Dvd / Film

394 Thuiswinkel Markt Monitor, p. 6.

395 Thuiswinkel Markt Monitor, p. 25.

Reizen	Kleding / Schoenen
Speelgoed	Overig

Tabel 4.1: Onderscheid van online marktsegmenten door BlauwResearch.

Ten behoeve van het empirisch onderzoek maak ik gebruik van de indeling van online marktsegmenten zoals die wordt gehanteerd door BlauwResearch, en zal het empirisch onderzoek worden verricht binnen de online marktsegmenten Verzekeringen, Reizen en Kleding/Schoenen.[396] De primaire overweging om het onderzoek uit te voeren binnen deze segmenten is gelegen in de omvang en diversiteit van de te verstrekken persoonsgegevens. Hiernaast is de keuze gebaseerd op de mate van gevoeligheid van de te verstrekken persoonsgegevens,[397] alsook op de mate van de georganiseerdheid van de segmenten en het toepassen van zelfregulering binnen die segmenten.

4.2.1 Omvang van de te verstrekken persoonsgegevens

Een eerste overweging bij de keuze van genoemde online marktsegmenten is de totale omvang van de door betrokkenen te verstrekken persoonsgegevens. Deze omvang kan worden gerelateerd aan het aantal bestellingen dat binnen de segmenten heeft plaatsgevonden en, zij het in mindere mate, de absolute omzet die is gegenereerd. Dit biedt een indicatie voor de omvang van het aantal persoonsgegevens dat jaarlijks door betrokkenen worden verstrekt in geval zij overgaan tot het online afnemen van producten. Ter indicatie: in 2009 zijn in totaal bijna 53,5 miljoen bestellingen geplaatst bij online winkels, een toename van 24% in vergelijking met 2008.[398]

Het online marktsegment Kleding is zowel in 2008 als 2009 het grootste segment indien wordt gemeten in het aantal online bestellingen per segment. In 2008 werden binnen dit segment in totaal 6,8 miljoen online bestellingen geplaatst, terwijl in 2009 het totaal aantal online bestellingen 9,4 miljoen bedroeg.[399]

De online verkopen zijn, gemeten in absolute omzet, zowel in 2008 en 2009 het hoogst in het online marktsegment Reizen. In 2008 lag de absolute omzet binnen dit segment boven de 1,9 miljard euro. In 2009 bedroeg de absolute omzet binnen het online marktsegment Reizen ruim 2,2 miljard euro.[400] Wat betreft het aantal bestellingen staat het marktsegment Reizen zowel in 2008 als 2009 met een derde plaats hoog gerangschikt; in 2008 bedroeg

396 In het vervolg zal dit segment worden aangeduid als het segment Kleding.

397 De term 'gevoelige gegevens' wordt ook gehanteerd in de MvT. Zie bijvoorbeeld Kamerstukken II 1997-1998, 25892, nr. 3, p. 22. Met de term 'gevoeligheid' wordt in dit kader ruimer ingezet dan de reikwijdte die in de Wbp/MvT wordt gehanteerd ten aanzien van gevoelige of bijzondere gegevens.

398 Thuiswinkel Markt Monitor, p. 22.

399 Thuiswinkel Markt Monitor, p. 30.

400 Thuiswinkel Markt Monitor, p. 26.

het aantal bestellingen 4,3 miljoen en in 2009 bedroeg het totaal aantal online bestellingen 5,4 miljoen.[401]

Het online marktsegment Verzekeringen staat, gemeten in absolute omzet, zowel in 2008 (367 miljoen euro) als 2009 (485 miljoen euro) op een derde plaats.[402] In 2009 zijn er in totaal 1,83 miljoen online verzekeringen afgesloten, een stijging van 38% vergeleken met 2008 (1,3 miljoen bestellingen).[403] BlauwResearch stelt in dit kader dat het segment Verzekeringen groot is qua omzet, maar een kleiner segment is in het aantal online bestellingen.[404]

4.2.2 Verstrekking van gevoelige persoonsgegevens

Een tweede overweging bij de keuze van genoemde online marktsegmenten is de mate van gevoeligheid van de persoonsgegevens die door de betrokkene aan de verantwoordelijke worden verstrekt. Een vluchtige verkenning op willekeurig gekozen websites van online verzekeraars en kleding- en reiswinkels leert dat de betrokkene in het online marktsegment Kleding bij aankoop van een product veelal zijn n.a.w.-gegevens, het nummer van zijn bankrekening en zijn e-mailadres aan de verantwoordelijke dient te verstrekken. In vergelijking met het online marktsegment Reizen zijn de door de betrokkene te verstrekken persoonsgegevens in het segment Kleding als minder gevoelig te kwalificeren. Immers, in het marktsegment Reizen dienen bijvoorbeeld persoonsgegevens over de samenstelling van het gezin of reisgezelschap, de vakantiebestemming, de duur van de vakantie, de beschikbare budgetten en gegevens van identiteitsbewijzen te worden verstrekt. In het online marktsegment Verzekeringen is de gevoeligheid van de te verstrekken persoonsgegevens het grootst. Zo dient de betrokkene bij het aanvragen of afsluiten van een autoverzekering gegevens over het type en de waarde van de te verzekeren auto, zijn n.a.w.-gegevens, gegevens over zijn beroep, de datum waarop hij zijn rijbewijs heeft gehaald, het aantal opgebouwde schadevrije jaren alsook over zijn bank- of gironummer te verstrekken. Tevens dient de betrokkene veelal te verklaren of een verzekeringsmaatschappij al dan niet een verzekering heeft opgezegd, geweigerd of tegen beperkende voorwaarden of verhoogde premie heeft geaccepteerd. In de meeste gevallen wordt tevens gevraagd naar een mogelijk strafrechtelijk verleden, wat betekent dat het hier om een bijzonder gegeven in de zin van de Wbp gaat. In het geval dat de betrokkene een zorgverzekering afsluit dient hij veelal zijn Burger Service Nummer, en dat van zijn eventueel mee te verzekeren gezinsleden, te verstrekken.

401 Thuiswinkel Markt Monitor, p. 30.
402 Thuiswinkel Markt Monitor, p. 26.
403 Thuiswinkel Markt Monitor Brancherapport segment Verzekeringen, p. 20.
404 Thuiswinkel Markt Monitor, p. 31.

4.2.3 De mate van georganiseerdheid en zelfregulering

De online marktsegmenten Verzekeringen, Reizen en Kleding kunnen worden onderscheiden naar de mate waarin deze segmenten zijn georganiseerd, en in het bijzonder zijn gereguleerd. De reden voor dit te hanteren onderscheid is gelegen in het feit dat hiermee wellicht een aanwijzing zou kunnen worden gevonden over een mogelijke relatie tussen zelfregulering enerzijds en de naleving van de informatieplicht aan de hand van een privacyverklaring anderzijds.

Het segment Verzekeringen is ten opzichte van de marktsegmenten Kleding en Reizen het sterkst middels zelfregulering vanuit de sector gereguleerd. Dit blijkt mede uit de lijst van 27 voor dit segment toepasselijke gedragscodes en keurmerken waarop de Tuchtraad Assurantiën toetst.[405] In paragraaf 2.3.3 is gerefereerd aan de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen. Op grond van deze gedragscode is een lid van het Verbond van Verzekeraars verplicht om op zijn website, via een privacyverklaring, informatie beschikbaar te stellen over het beleid met betrekking tot door middel van het Internet verkregen persoonsgegevens.[406] Daarentegen bleek dat bij het bepalen van de op te nemen inhoud wordt teruggevallen op de normen van artikel 33 lid 2 en 3 Wbp en artikel 34 lid 2 en 3 Wbp. Door in dit hoofdstuk empirisch vast te stellen of een online verzekeraar, die lid is van het Verbond van Verzekeraars, al dan niet uitvoering geeft aan zijn plicht om een privacyverklaring op zijn website te plaatsen en de betrokkene aan de hand hiervan te informeren over zijn beleid met betrekking tot de door middel van het Internet verkregen persoonsgegevens, kan wellicht een aanwijzing worden gevonden over een mogelijke wisselwerking tussen zelfregulering en de naleving van de informatieplicht.

Na het online marktsegment Verzekeringen volgt het online marktsegment Reizen waar het gaat om de invloed van zelfregulering. In dit segment is het met name de brancheorganisatie Algemene Nederlandse Vereniging van Reisorganisaties (ANVR) die de belangen van de reisorganisaties behartigt.[407] De ANVR is betrokken bij diverse reguleringsinitiatieven, waaronder het overleg in het kader van de Coördinatiegroep Zelfreguleringsoverleg van de SER op grond waarvan de ANVR Boekingsvoorwaarden en Reisvoorwaarden tot stand zijn gekomen.[408] Tevens is de ANVR, als representant van de reisbranche, partij geweest bij de totstandkoming van de Reclamecode

405 Dit overzicht is te vinden op de website van het Verbond van Verzekeraars: www.verbondvanverzekeraars.nl.

406 Artikel 10 Gedragscode Verwerking Persoonsgegevens Financiële Instellingen.

407 De ANVR omschrijft haar doelstelling als het bundelen van krachten van de aangesloten leden ten einde de gemeenschappelijke sociaal-economische belangen te behartigen, zodat de ANVR als organisatie nationaal en internationaal een toonaangevende plaats inneemt als vertegenwoordiger van de reisbranche.

408 ANVR-Boekingsvoorwaarden en ANVR-Reisvoorwaarden, zie aanhef.

Reisaanbiedingen.[409] Voorts heeft de ANVR een Huishoudelijk Reglement[410] en een Internetgedragscode[411] waaraan haar leden zich dienen te conformeren.

> ANVR Internetgedragscode, artikel 6. De wet- en regelgeving Gegevensbeheer en privacy.
> a. De reisonderneming zal persoonsgegevens behandelen conform de Wet Bescherming Persoonsgegevens (zie www.cbpweb.org). Dit houdt onder meer in dat de reisonderneming de daarvoor in aanmerking komende verwerking van persoonsgegevens aanmeldt bij het College Bescherming Persoonsgegevens.
> Als u de persoonsgegevens van klanten slechts verwerkt om een boeking uit te voeren hoeft geen melding plaats te vinden bij het College Bescherming Persoonsgegevens (art. 13 Vrijstellingsbesluit). Ook als de gegevens van de klant voor reclamedoeleinden worden gebruikt hoeft u zich niet aan te melden, mits aan de klant wordt aangegeven waarvoor zijn gegevens gebruikt worden (zie 6b) en de klant kan aangeven dat hij de reclame niet wil ontvangen (zie 6c). (WBP)
> b. De reisonderneming geeft duidelijk aan voor welk doel de persoonsgegevens worden gebruikt. (WBP)
> c. Als de persoonsgegevens ook worden gebruikt voor andere doelen dan de uitvoering van de reserveringsopdracht of boeking kan de reisonderneming - voor zover het gaat om eigen gelijkaardige producten of diensten - d.m.v. een 'opt-out' systeem de reiziger in staat stellen aan te geven dat geen toestemming wordt gegeven voor het toezenden van geadresseerd reclamemateriaal en/of het verstrekken van persoonsgegevens aan derden.
> Indien het niet gaat om eigen gelijkaardige producten of diensten dient de reisonderneming een 'opt-in' systeem te hanteren. (EH art. 15e, EC art. 13 en WBP)
> d. De reisonderneming biedt de reiziger de mogelijkheid om de toezending van geadresseerde (al dan niet elektronische) reclame op elk gewenst moment stop te zetten. De reisonderneming vermeldt de procedure daarvoor in of bij de toegezonden reclameuiting. (EC art. 13 en. WBP)
> e. De reisonderneming maakt duidelijk waar en op welke wijze de reiziger de geregistreerde persoonsgegevens kan inzien en desgewenst kan corrigeren of verwijderen. (WBP)

---

409 Deze code is van toepassing op reclame-uitingen en uitnodigingen tot aankoop gericht op de Nederlandse markt betreffende reisdiensten; Reclamecode Reisaanbiedingen d.d. 1 april 2009, punt 1. onder Definities.

410 Huishoudelijk Reglement ANVR (Algemene Nederlandse Vereniging van Reisondernemingen) ex. art 14 van de Statuten, Vastgesteld ALV 17.12.2009.

411 De ANVR Internetgedragscode kan worden geraadpleegd via de website van de ANVR: www.anvr.nl.

Wat betreft de verwerking van persoonsgegevens is specifiek artikel 6 van de ANVR Internetgedragscode relevant. In dit artikel wordt geen verplichting aan de leden opgelegd om een privacyverklaring op hun website op te nemen. Wel hebben de leden de plicht om de persoonsgegevens te behandelen conform de Wbp (artikel 6 sub a.), alsook om de betrokkenen te informeren over het doel waarvoor de persoonsgegevens worden gebruikt (artikel 6 sub b). Tevens wordt via dit artikel aan de leden de verplichting opgelegd om klanten te informeren over het recht op inzage, correctie, verwijderen en verzet (artikel 6 sub c. en e.). Het empirisch onderzoek kan mogelijk inzicht verschaffen in een relevant verschil tussen de naleving van de informatieplicht door een verantwoordelijke die lid is van de ANVR (en die tevens de ANVR Internetgedragscode dient na te leven) en de verantwoordelijke die geen lid is van de ANVR.

Het online marktsegment Kleding is ten opzichte van de segmenten Verzekeringen en Reizen het minst gereguleerd. In dit segment heeft de brancheorganisatie CBW-MITEX een voorname rol, zij het dat deze rol beperkter is in vergelijking met die van het Verbond van Verzekeraars of de ANVR. CBW-MITEX heeft een huishoudelijk reglement[412] waaraan leden zich dienen te conformeren, maar in dit reglement is geen verplichting voor de leden opgenomen om een privacyverklaring op hun website te plaatsen. Ook worden de leden niet anderszins verplicht om te handelen conform de Wbp. Navraag bij CBW-MITEX leert dat er geen overige reglementen of gedragscodes bestaan waarin deze verplichtingen zijn opgenomen. CBW-MITEX behartigt niet alleen de belangen voor de kledingbranche. Ook treedt ze op als belangenbehartiger voor de retail non-food branche. De rol die CBW-MITEX zichzelf toeschrijft is het adviseren en inspireren van leden, zodat ze optimaal rendement halen uit hun onderneming. Voorts verstrekt CBW-MITEX aan haar leden bedrijfs-, juridisch en personeelsadvies, geeft ze inzicht in marktcijfers en biedt zij leden hulp indien in geval van ondernemersvragen.[413]

Er wordt tenslotte op gewezen dat de geselecteerde online winkels tevens lid kunnen zijn van de belangenvereniging Thuiswinkel.org. Zoals bleek in paragraaf 2.2.3, is een voorwaarde voor het verkrijgen van een lidmaatschap van Thuiswinkel.org dat de verantwoordelijke een privacyverklaring op zijn website plaatst waarvan de inhoud is beoordeeld, en eventueel in overleg is aangepast, door een extern juridisch adviesbureau.

412 Huishoudelijk reglement CBW-MITEX, Goedgekeurd CBW-MITEX Ledenraad 30 maart 2010.

413 Zie ook de omschrijving op de website van CBW-MITX: www.cbwmitex.nl.

4.3 De selectie van de online winkels

Vanuit de keuze het empirisch onderzoek te verrichten binnen de segmenten online Verzekeraars, Reiswinkels en Kledingwinkels, worden de online winkels als volgt gedefinieerd:

Definities	Omschrijving
Online verzekeraar	Een verantwoordelijke die via zijn website verzekeringsproducten aanbiedt, en waarbij de betrokkene de mogelijkheid heeft om deze producten via die website aan te vragen of af te sluiten.[414]
Online reiswinkel	Een verantwoordelijke die via zijn website producten aanbiedt als vliegtickets, hotels, vakantiehuizen of packages, en waarbij de betrokkene de mogelijkheid heeft om deze producten via die website te reserveren en/of te boeken.[415]
Online kledingwinkel	Een verantwoordelijke die via zijn website producten aanbiedt als kleding, schoenen of accessoires, en waarbij de betrokkene de mogelijkheid heeft om deze producten via die website te kopen.

Tabel 4.2: Definitie van de online winkels.

De selectie van online verzekeraars is tot stand gekomen met behulp van vergelijkingssites over verzekeringen[416], de website van thuiswinkel.org, de website van het Verbond van Verzekeraars[417] en overige websites waarop online verzekeraars staan vermeld.[418] Dit resulteerde in totaal 57 online verzekeraars waar, via hun websites, een verzekeringsproduct kan worden aangevraagd of afgesloten. In het empirisch onderzoek wordt geen onderscheid gemaakt tussen het type verzekeraar en/of soort verzekeringsproduct.[419] Dit zou leiden tot een zodanig versnipperd beeld dat eventuele verschillen niet zijn te onderbouwen als statistisch significante verschillen. Voorts bevinden zich onder de populatie enkele online verzekeraars die eenzelfde moedermaatschappij

414 Uit een door mij uitgevoerde korte verkenning (voorafgaand aan de daadwerkelijke survey) naar 20 online verzekeraars volgt dat zowel bij het aanvragen als het afsluiten van een verzekeringsproduct (nagenoeg) dezelfde persoonsgegevens door de betrokkene dienen te worden verstrekt. Dit is reden om in het empirisch onderzoek geen onderscheid te maken tussen het online aanvragen of afsluiten van een verzekeringsproduct.

415 Uit een door mij uitgevoerde korte verkenning naar 35 online reiswinkels volgt dat zowel bij het reserveren als bij het boeken van een reisproduct (nagenoeg) dezelfde persoonsgegevens door de betrokkene dienen te worden verstrekt. Dit is reden om in het empirisch onderzoek geen onderscheid te maken tussen het online reserveren of boeken van een reisproduct.

416 Onder meer de sites www.verzekeringsite.nl, www.independer.nl, www.zorgkiezer.nl, www.verzekeringen-online.nl, www.onlineverzekeringen.com en www.prizewize.nl.

417 De website van het Verbond van Verzekeraars is: www.verbondvanverzekeraars.nl.

418 Onder meer de sites www.verzekeringen.startpagina.nl en www.onlineverzekeringen.eigenstart.nl.

419 Zoals bijvoorbeeld zorgverzekeraar, inkomensverzekeraar of schadeverzekeraar.

hebben, alsook zijn in het empirisch onderzoek online verzekeraars betrokken die diverse websites exploiteren, daarbij gebruikmakend van verschillende handelsnamen.[420] De reden dat deze online verzekeraars niet worden uitgesloten van het empirisch onderzoek is gelegen in het feit dat, hoewel er sprake is van één juridische entiteit, via de diverse websites veelal verschillende verzekeringsproducten worden aangeboden onder een apart label met een eigen identiteit en waar via elke website persoonsgegevens worden verkregen en verwerkt. Bovendien is het niet ondenkbaar dat, mede ten gevolge van diverse fusies en/of overnames, er verschil is in de vorm en/of inhoud van de privacyverklaringen die op die verschillende websites zijn opgenomen.

De 100 online reiswinkels die in de survey zijn betrokken werden geselecteerd met behulp van verzamelsites over online reiswinkels[421], de website van thuiswinkel.org, zoekmachines en overige websites waarop online reiswinkels staan vermeld. Er wordt binnen deze selectie geen onderscheid gemaakt in het type aanbieder[422] of het soort reisproduct dat door de online reiswinkel wordt aangeboden. [423]

De selectie van 100 online kledingwinkels is tot stand gekomen met behulp van verzamelsites over online kledingwinkels[424], de website van thuiswinkel.org, zoekmachines en overige websites waarop online kledingwinkels staan vermeld. Er wordt binnen deze selectie geen onderscheid gemaakt in het type kledingproduct[425], alsook wordt de omvang van de online kledingwinkel niet in het onderzoek betrokken.[426]

Voor een totaaloverzicht van de onderzochte webwinkels wordt verwezen naar Bijlagen A1, A2 en A3.

---

420 Een voorbeeld is bijvoorbeeld het bedrijf Achmea Schadeverzekeringen N.V. dat websites exploiteert onder de handelsnamen Zilveren Kruis Achmea, Groene Land Achmea, Avéro Achmea, FBTO, Centraal Beheer Achmea en InShared.

421 Onder meer de sites www.allereiswinkels.nl, www.alle-reiswinkels.com en vakantie.overzicht.nl.

422 Zoals bijvoorbeeld een onderscheid in reisbureau, touroperator of reisorganisatie.

423 Zoals bijvoorbeeld een onderscheid in groepsreizen of single reizen, wintersportvakantie of zomervakanties, accommodatie zoals hotel, chalet of bungalow.

424 Onder meer de sites www.vindallekleding.nl, www.kledingwinkels.nl en www.kledingonlinekopen.com.

425 Zoals bijvoorbeeld een onderscheid in heren-, dames- of kinderkleding.

426 Het maakt in dit onderzoek derhalve niet uit of de online kledingwinkel een eenmanszaak is, of dat de online kledingwinkel onderdeel uit maakt van een conglomeraat. Het hebben willen maken van een onderscheid in de omvang van online winkels zou tot gevolg hebben gehad dat alle onderzochte online winkels in alle segmenten moesten worden onderzocht in de registers van de Kamers van Koophandel. Daartoe ontbrak de benodigde tijd.

4.4 Vragenlijst

De in hoofdstuk 2 besproken opvattingen met betrekking tot het gebruik en de inhoud van privacyverklaringen hebben als basis gediend bij de ontwikkeling van een 1e concept vragenlijst. Dit 1e concept is toegepast op een totaal van 35 willekeurig gekozen websites van banken, verzekeringsmaatschappijen, reiswinkels, kledingwinkels en webwinkels met consumentenelektronica. Naar aanleiding hiervan zijn onderwerpen toegevoegd en zijn vragen aangescherpt en aangevuld, hetgeen heeft geleid tot een 2e concept vragenlijst. Dit tweede concept is vervolgens toegepast op een totaal van 20 willekeurig gekozen websites uit dezelfde segmenten als hiervoor genoemd. Naar aanleiding hiervan zijn nog enkele kleine wijzigingen doorgevoerd, waarna de definitieve vragenlijst werd vastgesteld. Onder de in totaal 55 willekeurig gekozen websites bevonden zich geen websites die onderwerp zijn van de uiteindelijke survey.
De inhoud van de privacyverklaringen van de in het onderzoek betrokken webwinkels zijn, zoals de vragenlijst laat zien, getoetst op zaken die niet als zodanig op grond van de Wbp verstrekt behoeven te worden. De doelstelling van het empirisch onderzoek is allereerst het helder krijgen op welke wijze exact de informatieplicht vorm en inhoud wordt gegeven waarbij niet uitsluitend wordt getoetst op het minimumniveau. Daarbij is het van belang te benadrukken dat de verantwoordelijke, op grond van de artikelen 33 en 34 Wbp, een onderwerp niet in een privacyverklaring hoeft te vermelden indien dit in het kader van de informatieplicht niet relevant is. Het feit dat in een privacyverklaring een bepaald onderwerp niet is opgenomen, behoeft daarmee als zodanig nog niets te zeggen. Tevens wordt met het onderzoek beoogd inzicht te verkrijgen in welke mate de elementen uit de door de Groep Gegevensbescherming Artikel 29 opgestelde lijst van minimaal te verstrekken informatie worden toegepast door verantwoordelijken. De vragenlijst is opgenomen in Bijlage B.

4.5 Statistische toets

De statistische vergelijking tussen en binnen de segmenten Verzekeringen, Reizen en Kleding heeft plaatsgevonden aan de hand van de chikwadraat toets. Met behulp van deze toets kan een statistisch significant verschil tussen de frequenties van voorkomen van twee of meer variabelen op nominaal niveau worden vastgesteld. Daarbij worden de waarden van de kenmerken tegen elkaar uitgezet in een kruistabel, zodat per cel de frequentie van voorkomen van iedere combinatie kan worden bepaald.[427]

[427] Voor meer uitleg over de chikwadraat toets zie Van der Zee, p. 126 e.v. en Baarda & De Goede, p. 307 e.v.

4.6 Onderzoeksperiode

Het verzamelen van de gegevens heeft plaatsgevonden in de periode van 7 juni 2010 tot en met 8 oktober 2010. Of een online winkel al dan niet lid is van het Verbond van Verzekeraars, de ANVR en/of de belangenorganisatie Thuiswinkel.org is vastgesteld aan de hand van de lidmaatschapsgegevens die op 21 juni 2010 stonden vermeld op de websites van de betreffende organisaties.

4.7 De aanwezigheid, vorm en kenbaarheid van de privacyverklaring

4.7.1 De aanwezigheid van de privacyverklaring

In 76% van alle gevallen heeft de online winkel een privacyverklaring op zijn website opgenomen, wat neerkomt op een totaal van 196 online winkels. In het segment Verzekeringen bedraagt dit percentage 95%, terwijl in het segment Reizen als in het segment Kleding 71% van de online winkels een privacyverklaring op zijn website heeft opgenomen.

Tabel 4.3	Totaal		Verzekeringen		Reizen		Kleding	
Heeft de online winkel een privacyverklaring op zijn website opgenomen?	n	%	n	%	n	%	n	%
Nee	61	23,7	3	5,3	29	29,0	29	29,0
Ja	196	76,3	54	94,7	71	71,0	71	71,0
			Pearson $\chi 2$= 13,8; df=2; p<.01					

De onderstaande analyses hebben betrekking op de 196 online winkels die een privacyverklaring op hun website hebben opgenomen.

4.7.2 De vorm van de privacyverklaring

In 92% van de gevallen wordt de privacyverklaring verstrekt aan de hand van een hyperlink. In 8% verschijnt de privacyverklaring met behulp van een pop up scherm, en wel nadat er handmatig op de button wordt geklikt. Er zijn geen voorbeelden waargenomen waarin een privacyverklaring werd verstrekt aan de hand van een vast tekstvenster of met behulp van een pop-up scherm dat automatisch verschijnt. Vermeld moet verder worden dat er geen significante verschillen waren te constateren tussen de segmenten Verzekeringen, Reizen en Kleding waar het de vorm van de privacyverklaring betreft.

Tabel 4.4	Totaal		Verzekeringen		Reizen		Kleding	
Wat is de verschijningsvorm van de privacyverklaring?	n	%	n	%	n	%	n	%
Hyperlink	181	92,3	51	94,4	63	88,7	67	94,4
Pop-up scherm dat verschijnt na een handmatige klik	15	7,7	3	5,6	8	11,3	4	5,6
Vast tekstvensters	0	0,0	0	0,0	0	0,0	0	0,0
Pop-up scherm dat automatisch verschijnt	0	0,0	0	0,0	0	0,0	0	0,0
Anders	0	0,0	0	0,0	0	0,0	0	0,0
			n.s.					

In 99% van alle gevallen wordt de privacyverklaring niet in een getrapte vorm gegeven. Er zijn geen significante verschillen tussen de segmenten Verzekeringen, Reizen en Kleding.

Tabel 4.5	Totaal		Verzekeringen		Reizen		Kleding	
Wordt de privacyverklaring in getrapte vorm gegeven?	n	%	n	%	n	%	n	%
Nee	194	99,0	52	96,3	71	100	71	100
Ja, in 2 treden	2	1,0	2	3,7	0	0,0	0	0,0
Ja, in 3 treden	0	0,0	0	0,0	0	0,0	0	0,0
Ja, in meer dan 3 treden	0	0,0	0	0,0	0	0,0	0	0,0
			n.s.					

4.7.3 De kenbaarheid van de privacyverklaring

De survey laat zien dat op 44% van de websites “privacy” de benaming is van de button van de hyperlink of pop up scherm, en in 19% wordt de term “privacystatement” gehanteerd. In het segment Verzekeringen gebruikt 56% de term “privacy” en 24% vermeldt “privacystatement”. In het segment Reizen gebruikt 50% de aanduiding “privacy” en 16% spreekt van “privacystatement”. In het segment Kleding ten slotte, zijn deze percentages respectievelijk 30% en 19%. Voorts is binnen dit segment in 21% van de gevallen de benaming van de hyperlink of pop up scherm “privacy policy”.

Tabel 4.6	Totaal		Verzekeringen		Reizen		Kleding	
Wat is de benaming van de button van de hyperlink of vaste pop up scherm?	n	%	n	%	n	%	n	%
Privacystatement	37	18,9	13	24,1	11	15,5	13	18,3
Privacyverklaring	12	6,1	0	0,0	5	7,0	7	9,9
Privacy	86	43,9	30	55,6	35	49,3	21	29,6
Mijn privacy	1	0,5	1	1,9	0	0,0	0	0,0

Privacy policy	21	10,7	1	1,9	5	7,0	15	21,1
Privacy reglement	1	0,5	0	0,0	0	0,0	1	1,4
Privacy en cookies verklaring	1	0,5	1	1,1	0	0,0	0	0,0
Privacybeleid	8	4,1	3	5,6	2	2,8	3	4,2
Uw privacy	4	2,0	2	3,7	1	1,4	1	1,4
Privacy en disclaimer	6	3,1	2	3,7	4	5,6	0	0,0
Anders	19	9,7	1	1,9	8	11,3	10	14,1
			Pearson $\chi 2$= 41,1; df=20; p<.01					

Verder laat het onderzoek zien dat in 24% van de websites de button van de hyperlink niet op de homepagina is geplaatst. Als we specifiek kijken naar het segment Reizen is dit percentage 35%, gevolgd door het segment Kleding met 25% en het segment Verzekeringen met 8%. In 72% van alle gevallen staat de button van de hyperlink onderaan de homepagina weergegeven. Voor het segment Verzekeringen is dit in 88% het geval, terwijl dit voor de segmenten Kleding en Reizen 67% respectievelijk 62% is.

Tabel 4.7	Totaal		Verzekeringen		Reizen		Kleding	
Is de button van de hyperlink op de home pagina weergegeven, en zo ja, wat is de positie van de button?	n	%	n	%	n	%	n	%
Nee	43	23,8	4	7,8	22	34,9	17	25,4
Ja, onderaan de homepagina	129	71,3	45	88,2	39	61,9	45	67,2
Ja, bovenaan de homepagina	5	2,8	2	3,9	1	1,6	2	3,0
Ja, aan de linker of rechterzijde van de Homepagina	4	2,2	0	0,0	1	1,6	3	4,5
			Pearson $\chi 2$=15,2; df=6; p<.05					

Bij 91% van alle webpagina's dient de betrokkene te scrollen alvorens de button van de hyperlink op de homepagina zichtbaar wordt. Er zijn op dit punt geen significante verschillen tussen de segmenten Verzekeringen, Reizen en Kleding.

Tabel 4.8	Totaal		Verzekeringen		Reizen		Kleding	
Is de button van de hyperlink zichtbaar zonder dat er gescrolled hoeft te worden?	n	%	n	%	n	%	n	%
Nee	165	91,2	43	84,3	60	95,2	62	92,5
Ja	16	8,8	8	15,7	3	4,8	5	7,5
			n.s.					

Indien er sprake is van een privacyverklaring die verschijnt met behulp van een pop-up scherm (nadat handmatig op de button wordt geklikt), is de button in 40% van de gevallen niet op de homepagina weergegeven. Indien de button wel op de homepagina staat, is bij 60% van de websites de positie van de button onderaan de homepagina. Ook hier zijn geen significante verschillen waar te nemen tussen de segmenten Verzekeringen, Reizen en Kleding.

Tabel 4.9	Totaal		Verzekeringen		Reizen		Kleding	
Is de button van het vaste pop-up scherm op de home pagina weergegeven, en zo ja, wat is de positie van de button?	n	%	n	%	n	%	n	%
Nee	6	40,0	0	0,0	3	37,5	3	75,0
Ja, onderaan de home pagina	9	60,0	3	100	5	62,5	1	25,0
Ja, bovenaan de homepagina	0	0,0	0	0,0	0	0,0	0	0,0
Ja, aan de linker of rechterzijde van de home pagina	0	0,0	0	0,0	0	0,0	0	0,0
			n.s.					

In 93% van alle gevallen moet de betrokkene scrollen alvorens de button van het pop-up scherm op de homepagina zichtbaar wordt. Wederom zijn geen significante verschillen tussen de segmenten Verzekeringen, Reizen en Kleding af te leiden.

Tabel 4.10	Totaal		Verzekeringen		Reizen		Kleding	
Is de button van het vaste pop-up scherm zichtbaar zonder dat er gescrolled hoeft te worden?	n	%	n	%	n	%	n	%
Nee	14	93,3	3	100	8	100	3	75,0
Ja	1	6,7	0	0,0	0	0,0	1	25,0
			n.s.					

4.7.4 Mogelijkheid tot opslaan van de privacyverklaring

Kijkend naar de vraag of de betrokkene de mogelijkheid wordt geboden om de privacyverklaring op te slaan (meer duurzaam vast te leggen) blijkt dat bij 91% van de websites de betrokkene deze mogelijkheid niet wordt geboden (met geen significante verschillen tussen de segmenten Verzekeringen, Reizen en Kleding).

Tabel 4.11	Totaal		Verzekeringen		Reizen		Kleding	
Kan de betrokkene de privacyverklaring opslaan?	n	%	n	%	n	%	n	%
Nee	178	90,8	48	88,9	66	93,0	64	90,1
Ja	18	9,2	6	11,1	5	7,0	7	9,9
			n.s.					

4.8 De inhoud van de privacyverklaring: verplichte elementen identiteit en doel van de verwerking

4.8.1 Verplicht element: identiteit van de verantwoordelijke

Op grond van de artikelen 33 lid 2 en 34 lid 2 Wbp is de verantwoordelijke verplicht nadere informatie over zijn identiteit te verstrekken. Bij het bepalen van de identiteit van de verantwoordelijke in de private sector is de formeel-juridische organisatie van de onderneming doorslaggevend, hetgeen betekent dat of de natuurlijke persoon of de rechtspersoon het rechtssubject is. In geval van een besloten of naamloze vennootschap dient derhalve de statutaire naam (inclusief de toevoeging BV of NV) van die rechtspersoon te worden vermeld. Waar het een eenmanszaak betreft, moet de naam van de natuurlijke persoon kenbaar worden gemaakt.[428]

De survey laat zien dat in 4,1% van de gevallen geen melding wordt gemaakt van de benodigde informatie over de identiteit van de verantwoordelijke. In het segment Kleding is dit percentage met 9% het grootst.

In 33% van alle gevallen wordt in de privacyverklaring de statutaire naam van de rechtspersoon vermeld. Het segment Verzekeringen scoort ten opzichte van de ander segmenten het hoogst; hier wordt in 59% van de gevallen in de privacyverklaring de statutaire naam vermeld.

In alle gevallen wordt niet de naam van de natuurlijke persoon als identiteit van de verantwoordelijke weergegeven. Dit is opmerkelijk aangezien zich onder de onderzochte websites eenmanszaken bevonden. Het had in die gevallen op de weg van de verantwoordelijke gelegen om zijn naam als natuurlijk persoon in de privacyverklaring te vermelden.

In 63% van alle gevallen wordt in de privacyverklaring weliswaar de identiteit van de verantwoordelijke genoemd, maar dan in de vorm van de handelsnaam. In het segment Reizen is dit percentage het hoogst (73%), gevolgd door het segment Kleding met 70%. In het segment Verzekeringen wordt in 39% van de gevallen de handelsnaam van de verantwoordelijke genoemd.

[428] Kamerstukken II 1997-1998, 25892, nr. 3, p. 56.

Tabel 4.12	Totaal		Verzekeringen		Reizen		Kleding	
Wordt de identiteit van de verantwoordelijke vermeld?	n	%	n	%	n	%	n	%
Nee	8	4,1	1	1,9	1	1,4	6	8,5
Ja, de naam van de natuurlijke	0	0,0	0	0,0	0	0,0	0	0,0
persoon	65	33,2	32	59,3	18	25,4	15	21,1
Ja, de statutaire naam van de	123	62,8	21	38,9	52	73,2	50	70,4
rechtspersoon								
Ja, de handelsnaam								
			Pearson χ^2= 27,5; df=4; p<.001					

4.8.2 Verplicht element: doel van de verwerking

Evenals informatie over zijn identiteit, dient de verantwoordelijke op grond van artikel 33 lid 2 en 34 lid 2 Wbp het doel van de verwerking vermelden. In 90% van alle onderzochte websites vermeldt de verantwoordelijke het doel van de verwerking in de privacyverklaring. In het segment Verzekeringen bedraagt dit percentage 98%, in het segment Reizen 85% en in het segment Kleding 90%.

Tabel 4.13	Totaal		Verzekeringen		Reizen		Kleding	
Wordt het doel van de verwerking vermeld?	n	%	n	%	n	%	n	%
Nee	19	9,7	1	1,9	11	15,5	7	9,9
Ja	177	90,3	53	98,1	60	84,5	64	90,1
			Pearson χ^2= 6,5; df=2; p<.05					

Overigens hoeft de verantwoordelijke op grond van artikel 33 lid 1 Wbp en artikel 34 lid 1 Wbp informatie over zijn identiteit dan wel het doel van de verwerking niet te vermelden indien de betrokkene daarvan reeds op de hoogte is. Het is niet ondenkbaar dat in de voornoemde situaties de verantwoordelijke deze informatie heeft opgenomen in zijn digitaal beschikbare algemene voorwaarden. Tevens zou het kunnen dat de bedoelde informatie elders op de website staat vermeld. Zo kan informatie over de identiteit van de verantwoordelijke bijvoorbeeld onder de button “contact” zijn vermeld. In paragraaf 4.11.2 zal dit aspect aan de orde komen.

4.9 De inhoud van de privacyverklaring: passieve informatieplicht

Bij 56% van alle onderzochte websites wordt melding gemaakt van het recht van de betrokkene op toegang tot de persoonsgegevens. In het segment Reizen wordt in 41% van de gevallen melding gemaakt van dit recht, in het segment Kleding is dit 58% en in het segment Verzekeringen 72%.

Tabel 4.14	Totaal		Verzekeringen		Reizen		Kleding	
Wordt melding gemaakt van het recht van de betrokkene op toegang tot de persoonsgegevens?	n	%	n	%	n	%	n	%
Nee	87	44,4	15	27,8	42	59,2	30	42,3
Ja	109	55,6	39	72,2	29	40,8	41	57,7
			Pearson χ^2= 12,4; df=2; p<.01					

In 76% van alle gevallen wordt melding gemaakt van het recht van de betrokkene om zich, afhankelijk van de situatie, te verzetten tegen de verwerking van persoonsgegevens. Het segment Kleding scoort hier met 80% het hoogst, gevolgd door het segment Verzekeringen (76%) en het segment Reizen (70%).

Tabel 4.15	Totaal		Verzekeringen		Reizen		Kleding	
Wordt melding gemaakt van het recht van de betrokkene om, afhankelijk van de situatie, zich te verzetten tegen de verwerking van persoonsgegevens?	n	%	n	%	n	%	n	%
Nee	48	24,5	13	24,1	21	29,6	14	19,7
Ja	148	75,5	41	75,9	50	70,4	57	80,3
			n.s.					

Op grond van artikel 36 lid 1 Wbp heeft de betrokkene het recht de hem betreffende persoonsgegevens te verbeteren, aan te vullen, te verwijderen en af te laten schermen. Dit recht komt de betrokkene slechts toe indien de persoonsgegevens feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.

Op 52% van de websites wordt melding gemaakt van het recht van de betrokkene op rectificatie van zijn persoonsgegevens. Dit percentage is met 65% het hoogst in het segment Verzekeringen, gevolgd door het segment Kleding (62%) en het segment Reizen (32%).

Tabel 4.16	Totaal		Verzekeringen		Reizen		Kleding	
Wordt melding gemaakt van het recht van de betrokkene op rectificatie van de persoonsgegevens?	n	%	n	%	n	%	n	%
Nee	94	48,0	19	35,2	48	67,6	27	38,0
Ja	102	52,0	35	64,8	23	32,4	44	62,0
			Pearson χ^2= 17,3; df=2; p<.001					

Kijkend naar het recht op verwijdering van de gegevens blijkt 26% van de onderzochte websites melding te maken van dit recht. In het segment Reizen is dit percentage 17%, in het segment Kleding 27% en in het segment Verzekeringen 37%.

Tabel 4.17	Totaal		Verzekeringen		Reizen		Kleding	
Wordt melding gemaakt van het recht van de betrokkene op verwijdering van de persoonsgegevens?	n	%	n	%	n	%	n	%
Nee	145	74,0	34	63,0	59	83,1	52	73,2
Ja	51	26,0	20	37,0	12	16,9	19	26,8
			Pearson χ^2= 6,5; df=2; p<.05					

4.10 De inhoud van de privacyverklaring: nadere informatie als waarborg voor een behoorlijke en zorgvuldige verwerking

4.10.1 Inleiding

In deze paragraaf zal inzichtelijk worden gemaakt welke nadere informatie in de praktijk door de verantwoordelijke zoal in privacyverklaringen wordt verstrekt als waarborg voor een behoorlijke en zorgvuldige verwerking.

4.10.2 Erkenning van het privacybelang van de betrokkene

Via de privacyverklaring vermeldt 70% van de onderzochte websites dat de verantwoordelijke belang hecht aan de privacy van de betrokkene. Voor de segmenten Verzekeringen en Reizen is dit 79%. Binnen het segment Kleding vermeldt 52% dat het privacybelang van betrokkenen wordt erkend.

Tabel 4.18	Totaal		Verzekeringen		Reizen		Kleding	
Wordt er vermeld dat de verantwoordelijke belang hecht aan de privacy van de betrokkene?	n	%	n	%	n	%	n	%
Nee	59	30,1	10	21,1	15	21,1	34	47,9
Ja	137	69,9	44	78,9	56	78,9	37	52,1
			Pearson χ^2= 16,8; df=2; p<.001					

4.10.3 Verwijzing naar de informatieplicht uit de Wbp

In alle gevallen wordt in de privacyverklaring niet expliciet opgemerkt dat de verantwoordelijke aan de hand van de privacyverklaring beoogt te voldoen aan de wettelijke informatieplicht.

Tabel 4.19	Totaal		Verzekeringen		Reizen		Kleding	
Wordt er vermeld dat de verantwoordelijke aan de hand van de privacyverklaring wil voldoen aan zijn informatieplicht die hij heeft op grond van de Wbp?	n	%	n	%	n	%	n	%
Nee	196	100	54	100	71	100	71	100
Ja	0	0,0	0	0,0	0	0,0	0	0,0
			n.s.					

4.10.4 Het fysieke en elektronische adres van de verantwoordelijke

In 21% van de onderzochte gevallen verstrekt de website informatie over het fysieke adres van de verantwoordelijke. In de segmenten Verzekeringen en Reizen bedraagt dit percentage in beide gevallen 15%. In het Segment Kleding wordt in 31% van de gevallen het fysieke adres van de verantwoordelijke vermeld. Daarbij dient te worden opgemerkt dat in dit onderzoek onder fysiek adres niet wordt verstaan een postbusnummer of een antwoordnummer.

Tabel 4.20	Totaal		Verzekeringen		Reizen		Kleding	
Wordt het fysieke adres van de verantwoordelijke vermeld?	n	%	n	%	n	%	n	%
Nee	155	79,1	46	85,2	60	84,5	49	69,0
Ja	41	20,9	8	14,8	11	15,5	22	31,0
			Pearson χ^2= 6,8; df=2; p<.05					

Het elektronische adres wordt in 46% van alle gevallen vermeld. In het segment Reizen is dit 56%, in het segment Kleding 51% en in het segment Verzekeringen 28%. Van belang is hier dat in dit onderzoek onder elektronisch adres niet wordt verstaan een webformulier.

Tabel 4.21	Totaal		Verzekeringen		Reizen		Kleding	
Wordt het elektronische adres van de verantwoordelijke vermeld?	n	%	n	%	n	%	n	%
Nee	105	53,6	39	72,2	31	43,7	35	49,3
Ja	91	46,4	15	27,8	40	56,3	36	50,7
			Pearson χ^2= 10,9; df=2; p<.01					

4.10.5 Verwerking van bijzondere gegevens

Opvallend zijn de uitkomsten waar het gaat om de verwerking van bijzondere persoonsgegevens. Van de onderzochte websites vermeldt of verduidelijkt 80% niet dat er bijzondere gegevens worden verwerkt. In slechts 9% wordt aangegeven dat er bijzondere gegevens worden verwerkt, en die gegevens zien op zowel medische als strafrechtelijke gegevens. Daarbij dient te worden genuanceerd dat er geen melding over de verwerking van bijzondere persoonsgegevens hoeft te worden gemaakt indien deze niet daadwerkelijk worden verwerkt. Binnen het segment Reizen geeft geen van de websites nadere informatie over een eventuele verwerking van bijzondere gegevens. Voor het segment Kleding geldt dit in 97% van de gevallen.

Binnen het segment Verzekeringen kaart 32% de eventuele verwerking van bijzondere persoonsgegevens niet via de privacyverklaring aan. In 33% van de gevallen wordt in het segment Verzekeringen wel vermeld of verduidelijkt dat er zowel medische als strafrechtelijke gegevens worden verwerkt en in 22% van de gevallen wordt vermeld of verduidelijkt dat er alleen medische gegevens worden verwerkt. Binnen dit segment maakt 9% melding van het feit dat er strafrechtelijke gegevens worden verwerkt.

Tabel 4.22	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld of verduidelijkt dat er bijzondere gegevens worden verwerkt?	n	%	n	%	n	%	n	%
Nee	157	80,1	17	31,5	71	100	69	97,2
Ja, er worden geen bijzondere gegevens verwerkt	1	0,5	0	0,0	0	0,0	1	1,4
Ja, er worden geen bijzondere gegevens verwerkt, tenzij met toestemming betrokkene	1	0,5	1	1,9	0	0,0	0	0,0
Ja, medische gegevens	12	6,1	12	22,2	0	0,0	0	0,0

Ja, strafrechtelijke gegevens	5	2,6	5	9,3	0	0,0	0	0,0
Ja, zowel medische als strafrechtelijke gegevens	18	9,2	18	33,3	0	0,0	0	0,0
Ja, maar niet nader verduidelijkt	2	1,0	1	1,9	0	0,0	1	1,4
			Pearson χ^2= 119,7; df=12; p<.001					

4.10.6 Verplichte of facultatieve verstrekking van persoonsgegevens

Op 96% van de websites wordt geen melding gemaakt van het feit of het verstrekken van de gevraagde persoonsgegevens verplicht of facultatief is. Voor het segment Kleding is dit 92%, voor het segment Reizen 97% en het segment Verzekeringen 100%.

Tabel 4.23	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld of het verstrekken van bepaalde informatie verplicht of facultatief is?	n	%	n	%	n	%	n	%
Nee	188	95,9	54	100	69	97,2	65	91,5
Ja	8	4,1	0	0,0	2	2,8	6	8,5
			Pearson χ^2= 6,1; df=2; p<.05					

4.10.7 Categorieën van ontvangers

Kijken we naar de categorieën van ontvangers, dan blijkt 84% van de onderzochte websites niet te vermelden voor welke (categorieën van) ontvangers binnen de organisatie van de verantwoordelijke de verzamelde persoonsgegevens bestemd zijn. Bij de segmenten Reizen en Kleding vermeldt geen van de websites hier iets over. In het segment Verzekeringen daarentegen wordt in 48% van de gevallen wel aangegeven voor welke (categorieën van) ontvangers de verzamelde persoonsgegevens bestemd zijn.

Tabel 4.24	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld voor welke ontvangers of categorieën van ontvangers binnen de organisatie van de verantwoordelijke de verzamelde persoonsgegevens bestemd is?	n	%	n	%	n	%	n	%
Nee	170	83,6	28	51,9	71	100	71	100
Ja	26	16,4	26	48,1	0	0,0	0	0,0
			Pearson χ^2= 78,8; df=2; p<.001					

4.10.8 Bewaartermijnen

Ook aan de bewaartermijn blijkt weinig aandacht te worden besteed: 93% van de websites geeft geen nadere informatie over de bewaartermijn van de verzamelde persoonsgegevens. Tussen de segmenten onderling zijn er op dit punt geen significante verschillen.

Tabel 4.25	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld hoe lang de bewaartermijn is van de verzamelde persoonsgegevens?	n	%	n	%	n	%	n	%
Nee	183	93,4	48	88,9	68	95,8	67	94,4
Ja	1	0,5	0	0,0	1	1,4	0	0,0
Ja, niet langer dan noodzakelijk is	12	6,1	6	11,1	2	2,8	4	5,6
			n.s.					

4.10.9 Beveiligingsmaatregelen

Meer aandacht is er wel voor de beveiligingsmaatregelen. In 54% van alle gevallen kaart de verantwoordelijke via de privacyverklaring het onderwerp beveiliging aan en stelt expliciet dat beveiligingsmaatregelen zijn getroffen om bijvoorbeeld de authenticiteit, integriteit en vertrouwelijkheid van de persoonsgegevens te waarborgen. In het segment Reizen is dit 42% van de gevallen, in het segment Kleding 52% en in het segment Verzekeringen 70%.

Tabel 4.26	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld of er beveiligingsmaatregelen zijn getroffen om bijvoorbeeld de authenticiteit van de website en/of de integriteit en vertrouwelijkheid van de via de website overgedragen persoonsgegevens te waarborgen?	n	%	n	%	n	%	n	%
Nee	91	46,4	16	29,6	41	57,7	34	47,9
Ja	105	53,6	38	70,4	30	42,3	37	52,1
			Pearson χ^2= 9,8; df=2; p<.01					

4.10.10 College bescherming persoonsgegevens en Functionaris voor de Gegevensbescherming

Kijken we naar het onderwerp melding bij het Cbp dan wel de functionaris gegevensbescherming, dan stellen we vast dat in 64% van alle gevallen hier niets over wordt gezegd. Bij 26% van de websites wordt de melding als zodanig wel aangekaart, maar wordt het nummer van de registratie van de melding niet via de privacyverklaring verstrekt.

Bij 10% van de onderzochte websites wordt wel melding gemaakt van zowel de melding bij het Cbp als het nummer van de registratie.

Kijken we op het specifieke niveau van de segmenten, dan stellen we ten aanzien van het segment Kleding vast dat in 86% van de gevallen niet via de privacyverklaring wordt aangekaart dat de verwerking is gemeld bij het Cbp. Bij het segment Reizen is dit 62%, terwijl het percentage voor het segment Verzekeringen 39% bedraagt. Een mogelijke verklaring voor het verschil is gelegen in het feit dat in de segmenten Kleding en Reizen mogelijk eerder een beroep kan worden gedaan op artikel 13 van het Vrijstellingenbesluit. Deze vrijstelling ziet op verwerkingen met betrekking tot bijvoorbeeld afnemers of leveranciers van de verantwoordelijke. Zo hoeven op grond van artikel 13 Vrijstellingenbesluit verwerkingen die zien op het doen van leveringen, bestellingen en het doen van betalingen onder dit artikel niet te worden gemeld. Ook mogen op grond van dit artikel de naam, de voorletters, het adres, de postcode, de woonplaats en soortgelijke voor communicatie benodigde gegevens waaronder ook het e-mailadres alsmede het bank- en/of girorekeningnummer van de betrokkenen worden verzameld.

Tabel 4.27	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld dat de verwerking is gemeld bij het Cbp?	n	%	n	%	n	%	n	%
Nee	126	64,3	21	38,9	44	62,0	61	85,9
Ja, inclusief het nummer van registratie	20	10,2	10	18,5	8	11,3	2	2,8
Ja, zonder nummer van registratie	50	25,5	23	43,6	19	26,8	8	11,3
			Pearson χ^2= 30,0; df=4; p<.001					

De verantwoordelijke heeft op grond van artikel 62 e.v. Wbp de mogelijkheid om een interne toezichthouder aan te stellen. Deze functionaris voor de gegevensbescherming (FG) houdt in dat geval binnen de organisatie van de verantwoordelijke toezicht op de toepassing en naleving van de Wbp. Meldingen van verwerkingen van persoonsgegevens zullen door de organisatie bij deze functionaris worden gedaan. Uit het onderzoek van Winter et al. volgt dat, gezien het grote aantal bedrijven, instellingen en andere organisaties in Nederland dat persoonsgegevens verwerkt, het aantal FG's bijzonder laag te noemen is.[429]

Bij 96% van de website is in de privacyverklaring niets te vinden over een eventuele melding bij de FG. In de segmenten Reizen en Kleding betreft dit percentage 100%. In het segment Verzekeringen is in 13% van de gevallen de verwerking gemeld bij een functionaris voor de gegevensbescherming.

[429] Winter et al., p. 63.

Tabel 4.28	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld dat de verwerking is gemeld bij een functionaris voor de gegevensbescherming?	n	%	n	%	n	%	n	%
Nee	189	96,4	47	87,0	71	100	71	100
Ja	7	3,6	7	13,0	0	0,0	0	0,0
			Pearson χ^2= 19,1; df=2; p<.001					

4.10.11 Contactpersonen in verband met de uitoefening van rechten of het hebben van vragen

Betrokkenen blijken in de meerderheid van de gevallen niet op de hoogte te worden gesteld van een eventueel aanspreekpunt bij de verantwoordelijke. Net iets meer dan 60% (concreet 61%) informeert betrokkenen niet over de naam en het adres tot wie zij zich kunnen wenden om rechten uit te oefenen. Bij 35% van de websites wordt de naam van een afdeling genoemd. Binnen het segment Reizen wordt in 85% van de gevallen niet vermeld tot wie de betrokkene zich moet wenden om zijn rechten uit te oefenen. Voor het segment Kleding bedraagt dit percentage 51% en voor het segment Verzekeringen is dit 44%. Kijken we naar het noemen van een naam van een afdeling, dat wordt in het segment Kleding in 49% een naam gegeven, in het segment Verzekeringen bedraagt dit 41% en in het segment Reizen 16%.

Tabel 4.29	Totaal		Verzekeringen		Reizen		Kleding	
Wordt melding gemaakt van de naam van de afdeling of functionaris tot wie de betrokkene zich moet wenden om zijn rechten uit te oefenen?	n	%	n	%	n	%	n	%
Nee	120	61,2	24	44,4	60	84,5	36	50,7
Ja, de Functionaris Gegevensbescherming	1	0,5	1	1,9	0	0,0	0	0,0
Ja, de naam van de privacy officer / coördinator	7	3,6	7	13,0	0	0,0	0	0,0
Ja, de naam van de afdeling	68	34,7	22	40,7	11	15,5	35	49,3
			Pearson χ^2= 43,6; df=6; p<.001					

In 63% van alle gevallen wordt niet de naam van de afdeling of functionaris vermeld die verantwoordelijk is voor het beantwoorden van vragen met betrekking tot de verwerking van persoonsgegevens. In het segment Reizen bedraagt dit percentage 85%, in het segment Kleding 54% en in het segment Verzekeringen 46%. Kijken we naar het segment Verzekeringen dan blijkt in 24% van de gevallen te worden verwezen naar een “privacy

officer" of "privacy coördinator". Binnen het segment Verzekeringen wordt in 24% van de gevallen de naam van een afdeling vermeld. Bij het segment Kleding is dit 47% en het segment Reizen 16%.

Tabel 4.30	Totaal		Verzekeringen		Reizen		Kleding	
Wordt de naam vermeld van de afdeling of functionaris die verantwoordelijk is voor het beantwoorden van vragen betreffende de verwerking van persoonsgegevens?	n	%	n	%	n	%	n	%
Nee	123	62,8	25	46,3	60	84,5	38	53,5
Ja, de Functionaris Gegevensbescherming	3	1,5	3	5,6	0	0,0	0	0,0
Ja, de naam van de privacy officer / coördinator	13	6,6	13	24,1	0	0,0	0	0,0
Ja, de naam van de afdeling	57	29,1	13	24,1	11	15,5	33	46,5
			Pearson χ^2= 63,1; df=6; p<.001					

4.10.12 Verstrekking van persoonsgegevens aan derden

Waar het informatie over derdenverstrekking betreft blijkt hier in de meerderheid van de gevallen aandacht voor te zijn. In 80% van de onderzochte websites wordt vermeld of persoonsgegevens al dan niet aan derden worden verstrekt. Het segment Kleding scoort hier het hoogst met 90%, gevolgd door de segmenten Reizen (89%) en Verzekeringen (56%). Daarbij dient te worden aangetekend dat is onderzocht of de privacyverklaring expliciet vermeldt of er al dan niet persoonsgegevens aan derden worden verstrekt.

Tabel 4.31	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld of persoonsgegevens al dan niet aan derden worden verstrekt?	n	%	n	%	n	%	n	%
Nee	39	19,9	24	44,4	8	11,3	7	9,9
Ja	157	80,1	30	55,6	63	88,7	64	90,1
			Pearson χ^2= 28,2; df=2; p<.001					

Kijken we naar een veelvoorkomende grondslag voor derdenverstrekking, namelijk wettelijke plicht, dan blijkt deze vrijwel nooit in aanvulling op het enkele feit van derdenverstrekking te worden vermeld: in 80% van de gevallen is dit niet het geval. Tussen de segmenten onderling zijn geen significante verschillen waar te nemen.

Tabel 4.32	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld of persoonsgegevens aan derden worden verstrekt op grond van een wettelijke plicht?	n	%	n	%	n	%	n	%
Nee	157	80,1	38	70,4	59	83,1	60	84,5
Ja	39	19,9	16	29,6	12	16,9	11	15,5
			n.s.					

Als het gaat om helderheid over de vraag aan welke derden dan exact gegevens worden verstrekt, blijken deze derden in 48% van alle gevallen specifiek te worden benoemd. In het segment Reizen betreft dit percentage 31%, in het segment Kleding 51% en in het segment Verzekeringen 67%.

Tabel 4.33	Totaal		Verzekeringen		Reizen		Kleding	
Worden er derden benoemd?	n	%	n	%	n	%	n	%
Nee	102	52,0	18	33,3	49	69,0	35	49,3
Ja	94	48,0	36	66,7	22	31,0	36	50,7
			Pearson χ^2= 16,0; df=2; p<.001					

In 96% van alle gevallen wordt niet vermeld dat persoonsgegevens, al dan niet mogelijk, aan derden in het buitenland worden verstrekt. In het segment Verzekeringen wordt in slechts 6% van de gevallen vermeld dat de persoonsgegevens naar derden buiten Europa worden verstrekt. Voor het segment Reizen als het segment Kleding is het in respectievelijk 1% en 3% niet duidelijk of de persoonsgegevens worden verstrekt naar derden in landen binnen dan wel buiten de Europa.

Tabel 4.34	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld dat de persoonsgegevens, al dan niet mogelijk, naar een derde in het buitenland worden verstrekt?	n	%	n	%	n	%	n	%
Nee	188	95,9	51	94,4	68	95,8	69	97,2
Ja, binnen Europa	0	0,0	0	0,0	0	0,0	0	0,0
Ja, buiten Europa	3	1,5	3	5,6	0	0,0	0	0,0
Ja, zowel binnen als buiten Europa	2	1,0	0	0,0	2	2,8	0	0,0
Ja, maar wordt niet nader gepreciseerd	3	1,5	0	0,0	1	1,4	2	2,8
			Pearson χ^2= 13,0; df=6; p<.05					

In 85% van alle gevallen wordt niet vermeld dat derden de vertrouwelijkheid en/of beveiliging van de persoonsgegevens garanderen. In het segment Kleding bedraagt dit percentage 75%, in het segment Reizen 97% en in het segment Verzekeringen 83%.

Tabel 4.35	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld dat derden de vertrouwelijkheid en/of beveiliging van de persoonsgegevens garanderen?	n	%	n	%	n	%	n	%
Nee	167	85,2	45	83,3	69	97,2	53	74,6
Ja, zowel vertrouwelijkheid en beveiliging	5	2,6	0	1,1	1	1,4	4	5,6
Ja, vertrouwelijkheid	24	12,2	9	16,7	1	1,4	14	19,7
Ja, beveiliging	0	0,0	0	0,0	0	0,0	0	0,0
			Pearson χ^2=17,4; df=4; p<.01					

4.10.13 Gebruik van cookies

Zoals besproken in hoofdstuk 2 is de informatieplicht uit de Wbp ook van toepassing indien de verantwoordelijke cookies wil plaatsen en uitlezen. Kijkend naar de wijze waarop deze plicht concreet via de onderzochte websites wordt ingevuld, blijkt dat in 70% van de gevallen expliciet melding wordt gemaakt van het feit dat de verantwoordelijke al dan niet gebruik maakt van cookies. Er zijn geen significante verschillen tussen de onderlinge segmenten. Er zij opgewezen dat, gezien de vraagstelling, niet kan worden vastgesteld of de verantwoordelijke daadwerkelijk gebruik maakt van cookies.

Tabel 4.36	Totaal		Verzekeringen		Reizen		Kleding	
Wordt melding gemaakt dat de verantwoordelijke al dan niet gebruik maakt van cookies?	n	%	n	%	n	%	n	%
Nee	58	29,6	12	22,2	22	31,0	24	33,8
Ja	138	70,4	42	77,8	49	69,0	47	66,2
			n.s.					

4.10.14 Betrokkenheid derden bij de totstandkoming van de privacyverklaring

In 100% van alle gevallen wordt in de privacyverklaring geen melding gemaakt of er derden betrokken zijn geweest bij de totstandkoming van de inhoud van de privacyverklaring.

Tabel 4.37	Totaal		Verzekeringen		Reizen		Kleding	
Wordt in de privacyverklaring melding gemaakt of er derden betrokken zijn geweest bij de totstandkoming van de inhoud van de privacyverklaring?	n	%	n	%	n	%	n	%
Nee	196	100	54	100	71	100	71	100
Ja	0	0,0	0	0,0	0	0,0	0	0,0
			n.s					

4.10.15 Gebondenheid aan gedragscode

Eerder in dit onderzoek is aangegeven dat binnen sommige sectoren de Wbp nader wordt ingevuld via het instrument van de gedragscode, en dat deze gedragscode soms melding kan maken van de inzet van een privacyverklaring ter voldoening aan de informatieplicht. In de privacyverklaring kan bovendien melding worden gemaakt van het bestaan van een eventuele gedragscode. De survey laat zien dat 78% van de websites via de privacyverklaring niet kenbaar maakt of de verantwoordelijke gebonden is, dan wel of hij zich gebonden acht, aan een gedragscode. Voor de segmenten Reizen en Kleding is dit percentage 100%. In het segment Verzekeringen wordt in 81% van de gevallen wel verklaard dat de verantwoordelijke gebonden is, dan wel zich gebonden acht, aan een gedragscode. Deze uitkomst is niet verrassend, aangezien alleen de verzekeringsbranche een gedragscode kent zoals bedoeld in artikel 25 Wbp.

Tabel 4.38	Totaal		Verzekeringen		Reizen		Kleding	
Wordt in de privacyverklaring verklaard of de verantwoordelijke gebonden is, dan wel zich gebonden acht, aan een gedragscode?	n	%	n	%	n	%	n	%
Nee	152	77,6	10	18,5	71	100,0	71	100,0
Ja, de verantwoordelijke is gebonden (verplicht)	10	5,1	10	18,5	0	0,0	0	0,0
Ja, de verantwoordelijke acht zich gebonden (vrijwillig)	0	0,0	0	0,0	0	0,0	0	0,0
Ja, maar niet duidelijk of dit een verplichting is of een eigen keuze	34	17,3	34	63,0	0	0,0	0	0,0
			Pearson χ^2= 149,2; df=4; p<.001					

In 19% van de gevallen binnen het segment Verzekeringen verklaart de verantwoordelijke dat hij gebonden is aan een gedragscode, waarbij uit de woordkeuze valt op te maken dat de gebondenheid voortvloeit uit een aan de verantwoordelijke opgelegde verplichting. In 63% van de gevallen verklaart de verantwoordelijke dat hij gebonden is aan een gedragscode, maar wordt niet duidelijk of die gebondenheid voortkomt uit een verplichting of dat het een keuze van de verzekeraar zelf is geweest.

In de gevallen waarin de verantwoordelijke gebonden is of zich gebonden acht aan een gedragscode kan in 52% van alle gevallen de betrokkene kennisnemen van de inhoud van die gedragscode via een hyperlink naar de site van de organisatie die de gedragscode heeft opgesteld. In 9% van de onderzochte gevallen wordt de gedragscode beschikbaar gesteld met behulp van een pdf-bestand.

Tabel 4.39	Totaal		Verzekeringen		Reizen		Kleding	
Indien ja, kan de betrokkene kennisnemen van de inhoud van die gedragscode en op welke wijze?	n	%	n	%	n	%	n	%
Nee	17	38,6	17	38,6	0	0,0	0	0,0
Ja, via een hyperlink naar de site van de organisatie die de gedragscode heeft opgesteld	23	52,3	23	52,3	0	0,0	0	0,0
Ja, via een PDF file	4	9,1	4	9,1	0	0,0	0	0,0
Ja, via een hyperlink die linkt naar een andere webpagina van de site van de verantwoordelijke	0	0,0	0	0,0	0	0,0	0	0,0
Ja, anders	0	0,0	0	0,0	0	0,0	0	0,0
			n.s.					

In alle gevallen (score 100%) dat binnen het segment Verzekeringen door de verantwoordelijke wordt vermeld dat hij gebonden is of zich gebonden acht aan een gedragscode, wordt concreet gerefereerd aan of gedoeld op de Gedragscode Financiële Instellingen.

Tabel 4.40	Verzekeringen	
Wordt gerefereerd aan of gedoeld op de Gedragscode Financiële Instellingen?	n	%
Nee	0	0,0
Ja	44	100

4.10.16 Akkoordverklaring en toestemming

In 98% van alle gevallen wordt in de privacyverklaring niet gefaciliteerd dat de betrokkene akkoord kan gaan met de inhoud van de privacyverklaring zodra hij zijn persoonsgegevens verstrekt dan wel concreet akkoord gaat met de inhoud van deze verklaring op het moment van het verstrekken van zijn gegevens.[430] In de segmenten Verzekeringen en Kleding bedraagt dit percentage 100%. In het segment Reizen is dit percentage 94%.

[430] Zie bijvoorbeeld de privacyverklaring van EBookers.nl: “Door persoonlijke informatie naar ons te verzenden en/of door gebruik te maken van onze website, stemt u ermee in dat wij zulke persoonlijke informatie mogen verzamelen, gebruiken en openbaar maken in overeenstemming met dit privacybeleid en voor zover wettelijk toegestaan of vereist. Als u niet met deze voorwaarden instemt, verstrek ons dan geen Persoonlijke Informatie”.

Tabel 4.41	Totaal		Verzekeringen		Reizen		Kleding	
Wordt in de privacyverklaring vermeld dat de betrokkene akkoord gaat met de inhoud van de privacyverklaring zodra hij zijn persoonsgegevens verstrekt?	n	%	n	%	n	%	n	%
Nee	192	98,3	54	100	67	94,4	71	100
Ja	4	1,7	0	0,0	4	5,6	0	0,0
			Pearson χ^2= 7,2; df=2; p<.05					

Eenzelfde hoog percentage (99%) komt naar voren als we kijken of de privacyverklaring melding maakt dat de betrokkene akkoord gaat met de inhoud van de privacyverklaring zodra hij zich op de website van de verantwoordelijke begeeft.[431] Er zijn geen significante verschillen geconstateerd tussen de segmenten onderling.

Tabel 4.42	Totaal		Verzekeringen		Reizen		Kleding	
Wordt in de privacyverklaring vermeld dat de betrokkene akkoord gaat met de inhoud van de privacyverklaring zodra hij zich op de website van de verantwoordelijke begeeft?	n	%	n	%	n	%	n	%
Nee	193	98,5	54	100	68	95,8	71	100
Ja	3	1,5	0	0,0	3	4,2	0	0,0
			n.s.					

In 75% van de onderzochte websites wordt in de privacyverklaring niets gezegd over het feit dat de betrokkene voor een specifieke verwerking toestemming moet geven of heeft gegeven aan de verantwoordelijke om zijn persoonsgegevens te mogen verwerken. In 24% van alle gevallen wordt dit wel vermeld, waarbij in dat geval wordt gesproken van “toestemming”. In 2% van de gevallen waarin dit wordt vermeld wordt gerefereerd aan “uitdrukkelijke toestemming”.

Als we specifiek kijken naar het segment Verzekeringen blijkt in 61% niet te worden vermeld dat de betrokkene voor de verwerking van zijn persoonsgegevens toestemming moet geven of heeft gegeven aan de verantwoordelijke. In het segment Kleding geldt dit voor 75% van de gevallen en in het segment Reizen bedraagt dit percentage 85%. In het segment Verzekeringen wordt in 37% wel vermeld dat de betrokkene toestemming aan de verantwoordelijke moet geven of heeft gegeven. In het segment Kleding betreft dit

[431] Zie bijvoorbeeld de privacyverklaring van SNP.nl: “Personen die de website snp.nl van SNP oproepen, verklaren dat ze met de onderstaande voorwaarden akkoord gaan”.

percentage 25% en in het segment Reizen 13%. In het segment Reizen wordt in 3% van de gevallen gesproken over “uitdrukkelijke toestemming” en in het segment Verzekeringen is hiervan sprake in 2%. Daarbij dient overigens te worden opgemerkt dat voor veel verwerkingen geen toestemming van de betrokkene benodigd zal zijn.

Tabel 4.43	Totaal		Verzekeringen		Reizen		Kleding	
Wordt in de privacyverklaring vermeld dat de betrokkene, al dan niet voor specifieke verwerkingen, toestemming moet geven of heeft gegeven aan de verantwoordelijke om zijn persoonsgegevens te mogen verwerken?	n	%	n	%	n	%	n	%
Nee	146	74,5	33	61,1	60	84,5	53	74,6
Ja, toestemming	47	24,0	20	37,0	9	12,7	18	25,4
Ja, ondubbelzinnige toestemming	0	0,0	0	0,0	0	0,0	0	0.0
Ja, uitdrukkelijke toestemming	3	1,5	1	1,9	2	2,8	0	0,0
			Pearson χ^2= 11,8; df=4; p<.05					

In 97% van alle gevallen wordt niet vermeld dat de betrokkene zijn gegeven toestemming te allen tijde kan intrekken. Tussen de segmenten onderling zijn er geen significante verschillen.

Tabel 4.44	Totaal		Verzekeringen		Reizen		Kleding	
Wordt vermeld dat de betrokkene zijn toestemming te alle tijden kan intrekken?	n	%	n	%	n	%	n	%
Nee	190	96,9	52	96,3	70	98,6	68	95,8
Ja	6	3,1	2	3,7	1	1,4	3	4,2
			n.s.					

Alhoewel de verwachting was dat geen van de privacyverklaringen expliciet iets zou vermelden over de in hoofdstuk 3 besproken situatie waarin een overeenkomst tot stand komt op basis waarvan persoonsgegevens worden verwerkt, zijn de websites hier toch op doorgenomen. Inderdaad blijkt dat in 100% van de gevallen geen melding in de privacyverklaring wordt gemaakt van de totstandkoming van een ‘privacyovereenkomst’ tussen de verantwoordelijke en de betrokkene.

Tabel 4.45	Totaal		Verzekeringen		Reizen		Kleding	
Wordt in de privacyverklaring verklaard of er wel of geen overeenkomt tussen de verantwoordelijke en de betrokkene tot stand komt?	n	%	n	%	n	%	n	%
Nee	196	100	54	100	71	100	71	100
Ja, er komt een overeenkomst tot stand	0	0,0	0	0,0	0	0,0	0	0,0
Ja, er komt geen overeenkomst tot stand	0	0,0	0	0,0	0	0,0	0	0,0
			n.s.					

4.10.17 (Rechts)maatregelen

Zoals in de voorgaande hoofdstukken besproken, kent zowel de Wbp als het BW diverse bepalingen die de betrokkene de mogelijkheid bieden zijn rechten te effectueren dan wel schadevergoeding te vorderen. Interessant is te bezien in hoeverre betrokkenen ook door de verantwoordelijken zelf, en wel via de privacyverklaring, op de hoogte worden gesteld van de verschillende rechtsmiddelen die hen ter beschikking staan. De analyse laat zien dat 87% van de onderzochte privacyverklaringen geen melding maakt van mogelijke rechtsmaatregelen die de betrokkene kan inzetten indien de verantwoordelijke jegens hem niet handelt conform de wettelijke of anderszins afgesproken regelingen. In 11% van alle gevallen wordt daar wel melding van gemaakt, waarbij in die gevallen er veelal specifiek op wordt gewezen dat een klacht moet worden ingediend bij de verantwoordelijke eventueel gevolgd door een bemiddelings- of klachtenprocedure bij een derde. Met betrekking tot het segment Verzekeringen wordt in 22% van de gevallen gewezen op de mogelijkheid tot het indienen van een klacht bij de verantwoordelijke waarbij die procedure eventueel gevolgd kan worden door een bemiddelings- of klachtenprocedure bij een derde.

Tabel 4.46	Totaal		Verzekeringen		Reizen		Kleding	
Wordt melding gemaakt welke (rechts)maatregelen de betrokkene kan treffen indien de verantwoordelijke tekortschiet in het verwerken van de persoonsgegevens of onrechtmatig handelt jegens de betrokkene?	n	%	n	%	n	%	n	%
Nee	171	87,2	38	70,4	70	98,6	63	88,7
Ja, indienen klacht bij de verantwoordelijke eventueel gevolgd door een bemiddelings- of klachtenprocedure bij een derde	21	10,7	12	22,2	1	1,4	8	11,3
Ja, rechtstreeks volgen van een bemiddelings- of klachtenprocedure bij een derde	3	1,5	3	5,6	0	0,0	0	0,0
Ja, rechtsmaatregelen bij de rechtbank	1	0,5	1	1,9	0	0,0	0	0,0
			Pearson χ^2= 25,8; df=6; p<.001					

4.10.18 Wijziging van de privacyverklaring

Gegeven het feit dat privacyverklaringen door sommige bedrijven lopende de tijd hun privacyverklaring aanpassen (wat bijvoorbeeld grote internationale sociale netwerk sites en zoekmachines blijken te doen), is het interessant te bezien in hoeverre de in dit onderzoek bekeken websites het recht voorbehouden de privacyverklaring aan te passen. In 48% van de gevallen blijkt de verantwoordelijke zich het recht voor te behouden om de inhoud van de privacyverklaring eenzijdig te wijzigen. In het segment Reizen is dit percentage 27%, in het segment Kleding 47% en in het segment Verzekeringen 78%.

Tabel 4.47	Totaal		Verzekeringen		Reizen		Kleding	
Behoudt de verantwoordelijke zich het recht voor om de inhoud van de privacyverklaring eenzijdig te wijzigen?	n	%	n	%	n	%	n	%
Nee	102	52,0	12	22,2	52	73,2	38	53,5
Ja	94	48,0	42	77,8	19	26,8	33	46,5
			Pearson χ^2= 32,1; df=2; p<.001					

In de gevallen dat de verantwoordelijke zich het recht voorbehoudt om de inhoud van de privacyverklaring eenzijdig te wijzigen, blijkt in 71% van de gevallen dat de betrokkene zelf actief de privacyverklaring regelmatig op de website moet raadplegen om te kunnen

beoordelen of er wijzigingen hebben plaatsgevonden. In 20% van alle gevallen wordt de betrokkene wel door de verantwoordelijke geïnformeerd dat de verklaring is aangepast. In het segment Kleding dient de betrokkene in 61% van de gevallen de privacyverklaring op de website zelf te raadplegen. In het segment Reizen is dit percentage 63% en in het segment Verzekeringen 83%.
De betrokkene wordt in het segment Kleding in 40% van de gevallen door de verantwoordelijke geïnformeerd dat de inhoud van de privacyverklaring is gewijzigd. In het segment Reizen gebeurt dit in 21% en in het segment Verzekeringen in 5% van de gevallen.

Tabel 4.48	Totaal		Verzekeringen		Reizen		Kleding	
Indien ja, op welke wijze wordt de betrokkene geïnformeerd in geval van wijzigingen van de privacyverklaring	n	%	n	%	n	%	n	%
De betrokkene dient zelf de privacyverklaring op de website regelmatig te raadplegen	67	71,3	35	83,3	12	63,2	20	60,6
De verantwoordelijke informeert de betrokkene	19	20,2	2	4,8	4	21,1	13	39,4
Wordt niet nader geregeld	8	8,5	5	11,9	3	15,8	0	0,0
			Pearson χ^2= 17,1; df=4; p<.01					

4.11 De privacyverklaring en elektronische algemene voorwaarden

4.11.1 Elektronische algemene voorwaarden

Omdat bepaalde informatie die vanuit de Wbp dient te worden verstrekt niet per se via een privacyverklaring tot de betrokkene behoeft te komen, maar ook via elektronische algemene voorwaarden is tevens onderzocht of de verantwoordelijke, behalve een privacyverklaring, ook elektronische algemene voorwaarden op zijn website heeft geplaatst. In 93% van alle gevallen blijkt dit het geval te zijn. Het segment Kleding scoort hier met 96% het hoogst, gevolgd door het segment Reizen (93%) en het segment Verzekeringen (86%).

De naam voor de button (link) waar de elektronische algemene voorwaarden op de website achter te vinden zijn is in het segment Verzekeringen in 70% van de gevallen ‘disclaimer’.
In het segment Reizen heeft de verantwoordelijke in 31% van de gevallen twee buttons op zijn website geplaatst, te weten een button met de naam ‘algemene voorwaarden’ en een button geheten ‘disclaimer’. In 25% van de gevallen is er in het segment Reizen een button met de aanduiding ‘disclaimer’, en in 19% van de gevallen een button waarop ‘algemene voorwaarden’ staat vermeld.

De verantwoordelijke heeft in het segment Kleding in 69% van de gevallen een button op de website geplaatst onder de naam ‘algemene voorwaarden’.

Tabel 4.49	Totaal		Verzekeringen		Reizen		Kleding	
Zijn er, naast de privacyverklaring, elektronische algemene voorwaarden?	n	%	n	%	n	%	n	%
Nee	19	7,4	8	14,0	7	7,0	4	4,0
Ja, onder de naam algemene voorwaarden	88	34,2	0	0,0	19	19,0	69	69,0
Ja, onder de naam disclaimer	65	25,3	40	70,2	25	25,0	0	0,0
Ja, onder de naam juridische informatie	4	1,6	2	3,5	1	1,0	1	1,0
Ja, maar andere naam	39	15,2	3	5,3	17	17,0	19	19,0
Ja, zowel algemene voorwaarden als Disclaimer	42	16,3	4	7,0	31	31,0	7	7,0
			Pearson $\chi 2=165,5$; df=10; p<.001					

Bij 71% van de websites zijn in de elektronische algemene voorwaarden geen bepalingen opgenomen die zien op de verwerking van persoonsgegevens. In het segment Verzekeringen is dit percentage 90%, gevolgd door het segment Reizen (79%) en het segment Kleding (54%).

Daar waar in de elektronische algemene voorwaarden bepalingen omtrent de verwerking van persoonsgegevens zijn opgenomen, blijken die bepalingen in alle segmenten voornamelijk materieel van aard. In het segment Kleding is dat in 40% van de gevallen, gevolgd door het segment Reizen (17%) en het segment Verzekeringen (8%).

Tabel 4.50	Totaal		Verzekeringen		Reizen		Kleding	
Zijn er in de algemene voorwaarden bepalingen opgenomen die zien op de verwerking van persoonsgegevens?	n	%	n	%	n	%	n	%
Nee	169	71,0	44	89,8	73	78,5	52	54,2
De bepalingen zijn materieel van aard	58	24,4	4	8,2	16	17,2	38	39,6
Er wordt bepaald dat de privacyverklaring onderdeel uit maakt van de algemene voorwaarden	0	0,0	0	0,0	0	0,0	0	0,0
Er wordt bepaald dat de privacyverklaring van toepassing is in geval van verwerkingen van persoonsgegevens, maar de (mogelijke) verhouding tussen elektronische algemene voorwaarden en de privacyverklaring wordt niet verduidelijkt	11	4,6	1	2,0	4	4,3	6	6,3
			Pearson $\chi 2$=24,6; df=6; p<.001					

4.11.2 Identiteit en doel van de verwerking in elektronische algemene voorwaarden of elders op de website

De verantwoordelijke behoeft op grond van artikel 33 lid 1 Wbp en artikel 34 lid 1 Wbp geen informatie over zijn identiteit of over het doel van de verwerking te vermelden indien de betrokkene daarvan reeds op de hoogte is. Gekeken is of de verantwoordelijke die in de privacyverklaring geen informatie over de identiteit of het doel van de verwerking heeft vermeld, deze elementen wel heeft opgenomen in elektronische algemene voorwaarden, of dat deze elementen elders op de website worden vermeld. Aldus zijn er 2 scenario's te onderscheiden.

In Scenario 1 heeft de verantwoordelijke zowel een privacyverklaring als elektronische algemene voorwaarden op zijn website geplaatst. In de privacyverklaring wordt echter geen informatie over de identiteit dan wel het doel van de verwerking vermeld. In dat geval is bekeken of deze ontbrekende informatie wel via de elektronische algemene voorwaarden wordt verstrekt. Indien dit het geval was, is niet verder onderzocht of deze informatie elders op de website stond vermeld. Indien de genoemde informatie niet in de elektronische algemene voorwaarden waren opgenomen, is onderzocht of deze elders op de website stond vermeld.

In Scenario 2 heeft de verantwoordelijke wel een privacyverklaring maar geen elektronische algemene voorwaarden op zijn website geplaatst. In de privacyverklaring wordt echter geen informatie over de identiteit of het doel van de verwerking gegeven. In dat geval is onderzocht of de ontbrekende informatie elders op de website was te vinden. Uit het onderzoek volgt dat in slechts een enkel geval sprake was van Scenario 2. Derhalve wordt

een verdere bespreking van dit scenario hier achterwege gelaten, en voor de resultaten verwezen naar tabel 4.51 (identiteit) en tabel 4.52 (doel van de verwerking).

Specifiek voor wat betreft Scenario 1 in relatie tot informatie over de identiteit van de verantwoordelijke is het volgende uit het onderzoek af te leiden. Voor het segment Verzekeringen geldt dat in de gevallen waar de verantwoordelijke geen informatie over zijn identiteit in de privacyverklaring heeft opgenomen, in 10% daarvan hij deze informatie wel vermeldt in elektronische algemene voorwaarden. In 40% van die gevallen staat de informatie elders op de website vermeld.
Voor wat betreft het segment Reizen geldt dat in die gevallen dat de verantwoordelijke geen informatie over zijn identiteit in de privacyverklaring heeft opgenomen, in 40% daarvan hij deze informatie wel geeft in de elektronische algemene voorwaarden, en in 8% van die gevallen deze informatie elders op de website staat vermeld.
Tenslotte laat het onderzoek zien dat in het segment Kleding in 29% van de gevallen de informatie over identiteit van de verantwoordelijke wel in elektronische algemene voorwaarden staat vermeld, en in 6% van de gevallen deze informatie elders op de website is opgenomen.

Tabel 4.51	Totaal		Verzekeringen		Reizen		Kleding	
Geen identiteit van de verantwoordelijke in de privacyverklaring, maar mogelijk wel in AV of elders op de website	n	%	n	%	n	%	n	%
Scenario 1: Wel een PV en wel AV								
Identiteit vermeld in de AV	39	30,7	2	10,0	21	40,4	16	29,0
Identiteit vermeld elders op de website	15	11,8	8	40,0	4	7,7	3	5,5
Identiteit niet vermeld in AV of elders op de website	73	57,5	10	50,0	27	51,9	36	65,5
Scenario 2: Wel een PV en geen AV								
Identiteit vermeld elders op de website	1	25,0	0	0,0	0	0,0	1	100,0
Identiteit niet vermeld elders op de website	3	75,0	2	100,0	1	100,0	0	0,0

Kijkend vanuit Scenario 1 naar vermelding van het doel van de verwerking valt het volgende te constateren (zie tabel 4.52). Voor het segment Verzekeringen geldt ten aanzien van het ene specifieke geval waarin de verantwoordelijke het doel van de verwerking niet in de privacyverklaring had opgenomen, hij dit doel wel elders op de website kenbaar maakte.
Voor het segment Reizen geldt dat in die gevallen dat de verantwoordelijke het doel van de verwerking niet heeft opgenomen in de privacyverklaring, in 9% van die gevallen hij het doel van de verwerking wel heeft vermeld in elektronische algemene voorwaarden, en in geen van de gevallen het doel elders op de website staat vermeld.
Ten slotte volgt uit het onderzoek dat in het segment Kleding in 29% van de gevallen het doel van de verwerking door de verantwoordelijke is vermeld in elektronische algemene voorwaarden, en in geen van de gevallen het doel elders op de website staat vermeld.

Tabel 4.52	Totaal		Verzekeringen		Reizen		Kleding	
Geen doel van de verantwoordelijke in de privacyverklaring, maar mogelijk wel in AV of elders op de website	n	%	n	%	n	%	n	%n
Scenario 1: Wel een PV en wel AV								
Doel vermeld in de AV	3	15,8	0	0,0	1	9,1	2	28,6
Doel vermeld elders op de site	1	5,3	1	100,0	0	0,0	0	0,0
Doel niet vermeld in AV of elders op de website	15	78,9	0	0,0	10	90,9	5	71,4
Scenario 2: Wel een PV en geen AV								
Doel vermeld elders op de site	0	0,0	0	0,0	0	0,0	0	0,0
Doel niet vermeld elders op de website	0	0,0	0	0,0	0	0,0	0	0,0

4.12 Lidmaatschap van een belangenorganisatie

4.12.1 Lidmaatschap: Segment Verzekeringen

Zoals toegelicht in paragraaf 4.3 vond het empirisch onderzoek plaats onder 57 online verzekeraars. Deze online verzekeraars kunnen lid zijn van het Verbond van Verzekeraars, van Thuiswinkel.org alsook van beide belangenorganisaties.

Allereerst is onderzocht of er statistisch significante verschillen optreden ten aanzien van het gebruik van een privacyverklaring indien een online verzekeraar lid is van het Verbond van Verzekeraars. Voor de relevante kruistabellen die een onderling statistisch significant verschil laten zien, wordt verwezen naar Bijlage C1.

Vervolgens is onderzocht of er statistisch significante verschillen waar te nemen zijn ten aanzien van het gebruik van een privacyverklaring indien een online verzekeraar lid is van Thuiswinkel.org. Voor de betreffende kruistabellen wordt verwezen naar Bijlage C2.

Uit het onderzoek kan worden geconcludeerd dat het uitmaakt of de online verzekeraar lid is van het Verbond van Verzekeraars: er zijn vrij veel statistisch significante verschillen. Bovendien kan worden geconcludeerd dat het nauwelijks relevant is of de online verzekeraar lid is van Thuiswinkel.org: er zijn hier nauwelijks statistisch significante verschillen waar te nemen.

Omdat de online verzekeraar lid kan zijn van zowel het Verbond van Verzekeraars als van Thuiswinkel.org, is onderzocht of statistisch significante verschillen optreden indien de 57 online verzekeraars worden onderscheiden naar 4 categorieën, te weten:

1. De online verzekeraar die noch lid is van het Verbond van Verzekeraars noch van Thuiswinkel.org.
2. De online verzekeraar die uitsluitend lid is van het Verbond van Verzekeraars.
3. De online verzekeraar die uitsluitend lid is van Thuiswinkel.org.
4. De online verzekeraar die zowel lid is van het Verbond van Verzekeraars als van Thuiswinkel.org.

Aangetekend moet worden dat de onderverdeling in 4 categorieën tot gevolg heeft dat iedere groep, vanuit statistisch oogpunt bekeken, een beperkt aantal online verzekeraars omvat. Dit heeft tot gevolg dat resultaten weliswaar statistisch significante verschillen laten zien, maar vanwege de beperkte omvang slechts als indicatief moeten worden beschouwd. Voor de hier relevante kruistabellen die een onderling statistisch significant verschil laten zien wordt verwezen naar Bijlage C3. De resultaten worden hierna besproken.

Identiteit

Indien een online verzekeraar geen lid is van een belangenorganisatie, wordt in 24% de statutaire naam van de verantwoordelijke genoemd. Is de online verzekeraar lid van het Verbond van Verzekeraars, dan wordt in 81% de statutaire naam genoemd. Is de online verzekeraar lid van Thuiswinkel.org, dan vermeldt 50% de statutaire naam. In het geval de online verzekeraar lid is van zowel het Verbond van Verzekeraars als Thuiswinkel.org, wordt in alle gevallen (100%) de statutaire naam als identiteit vermeld.

Recht op toegang tot de persoonsgegevens

Indien een online verzekeraar geen lid is van een belangenorganisatie, wordt in 47% vermeld dat de betrokkene recht heeft op toegang tot zijn persoonsgegevens. Indien de online verzekeraar lid is van het Verbond van Verzekeraars bedraagt dit percentage 81%, en bij het lidmaatschap van Thuiswinkel.org is dit percentage 83%. In het geval de online

verzekeraar zowel lid is van het Verbond van Verzekeraars als van Thuiswinkel.org, is de score met 89% het hoogst.

Fysieke adres van de verantwoordelijke
Uit paragraaf 4.10.4 volgde dat het segment Verzekeringen ten opzichte van de segmenten Reizen en Kleding het laagst scoort met betrekking tot het vermelden van het fysieke adres. Indien een online verzekeraar lid is van Thuiswinkel.org, wordt in 42% het fysieke adres genoemd. Dit percentage bedraagt 6% indien de online verzekeraar geen lid is van een belangenorganisatie.

Verwerking van bijzondere gegevens
Indien een online verzekeraar geen lid is van een belangenorganisatie, wordt in 59% van de gevallen in de privacyverklaring melding gemaakt dat er bijzondere gegevens worden verwerkt. Indien de online verzekeraar lid is van het Verbond van Verzekeraars bedraagt dit percentage 81%. Het percentage is het hoogst (100%) waar de online verzekeraar lid is van zowel het Verbond van Verzekeraars als Thuiswinkel.org.

Stichting CIS
Bij de inhoudelijke beoordeling van de privacyverklaringen binnen het segment Verzekeringen viel op dat in een aantal gevallen werd verwezen naar de database van de Stichting Centraal Informatie Systeem (CIS). Deze stichting bewaart verzekeringsgegevens voor in Nederland werkzame verzekeringsmaatschappijen. Tevens behartigt de stichting de belangen van de deelnemers door verwerking van informatie die kan worden gebruikt bij het schatten van te verzekeren risico's en het beheersen van de schadelast door een verantwoord acceptatiebeleid. Een ander doel van de Stichting CIS is het verwerken van informatie die belangrijk is ten aanzien van het voorkomen en bestrijden van verzekeringscriminaliteit. De registraties die de Stichting CIS hiertoe voert zien op (i) schademeldingen, (ii) eigenaren en bestuurders van een onverzekerd motorvoertuig dat betrokken is geweest bij een aanrijding, (iii) opzegging van verzekeringsproducten door de verzekeraar en (iv) ontzeggingen van de rijbevoegdheid.[432] Een betrokkene kan derhalve, zij het indirect, met de Stichting CIS van doen krijgen indien hij een verzekering aanvraagt of als hij een schadeclaim indient bij zijn verzekeraar. Anders gezegd, de Stichting CIS verwerkt naar alle waarschijnlijkheid persoonsgegevens van de betrokkene die door de verzekeraar aan de Stichting CIS zijn verstrekt. In dat kader is in het empirisch onderzoek bekeken of, en zo ja wat, door de verzekeraar in de privacyverklaring wordt vermeld over de Stichting CIS.

[432] Een meer uitgebreide beschrijving over de Stichting Centraal Informatie Systeem en de doelen van de verwerkingen, is te vinden op de website www.stichtingcis.nl.

Uit onderzoek volgt dat in 46% van de gevallen in de privacyverklaring wordt vermeld dat de verantwoordelijke gebruik maakt van de databases van de Stichting CIS. Van deze gevallen wordt in 8% niet verduidelijkt op welke wijze de verantwoordelijke hiervan gebruik maakt. In alle overige gevallen (92%) vermeldt de verantwoordelijke dat hij de database gebruikt voor het raadplegen van persoonsgegevens van de betrokkene. Er wordt in geen van de gevallen door de verantwoordelijke vermeld dat hij persoonsgegevens of overige gegevens verstrekt aan de Stichting CIS. Dit is opmerkelijk aangezien de database van de Stichting CIS mede wordt gevuld met (persoons)gegevens die afkomstig zijn van de verzekeraars.
In 96% wordt door de verantwoordelijke verwezen naar de privacyverklaring van de Stichting CIS, maar de verhouding tussen de privacyverklaring van de verantwoordelijke enerzijds en die van de Stichting CIS anderzijds wordt niet verduidelijkt. Tot slot wordt in 48% van de gevallen in de privacyverklaring vermeld dat de leden van de Stichting CIS onderling gegevens uitwisselen. Dit is opvallend nu de noodzaak om onderling gegevens te doen uitwisselen zou moeten ontbreken juist vanwege het bestaan van de Stichting CIS. Desgevraagd verduidelijkt de Stichting CIS dat de deelnemers zelf verantwoordelijk zijn voor de vastlegging van door hen ontvangen claimmeldingen en voor correcte toepassing van de CIS databank in hun dagelijkse werkzaamheden. “Door bevragingen uit te voeren op de databank kunnen deelnemers kennis nemen van registraties van andere deelnemers. De onderlinge uitwisseling van verzekeringsgerelateerde gegevens tussen onze deelnemers vindt dus plaats door middel van de centrale databank die Stichting CIS beheert. Wellicht zou de desbetreffende mededeling over informatie-uitwisseling duidelijker zijn als deze luidt: Deelnemers van Stichting CIS wisselen onder meer via een centrale databank onderling informatie uit”.[433]
Voor de relevante kruistabellen met betrekking tot de bovengenoemde bevindingen ten aanzien van Stichting CIS wordt verwezen naar Bijlage D.

Indien een online verzekeraar geen lid is van een belangenorganisatie, blijkt in 88% geen melding te worden gemaakt van het feit of de verantwoordelijke gebruik maakt van de Stichting CIS. Indien de online verzekeraar lid is van het Verbond van Verzekeraars bedraagt dit percentage 69%. Het percentage is het hoogst (100%) indien de online verzekeraar lid is van zowel het Verbond van Verzekeraars als Thuiswinkel.org.

4.12.1.1 Conclusie met betrekking tot het segment Verzekeringen

Uit het voorgaande volgt dat, ten aanzien van het gebruik van een privacyverklaring, het binnen het segment Verzekeringen uitmaakt of de online verzekeraar lid is van een belangenorganisatie. Daarbij lijkt een lidmaatschap van het Verbond van Verzekeraars op dit punt meer bepalend te zijn dan een lidmaatschap van Thuiswinkel.org.

[433] Correspondentie tussen Stichting CIS en E.W. Verhelst, d.d. 5 oktober 2011.

Het is opmerkelijk dat de groep online verzekeraars die geen lid is van een belangenorganisatie op twee onderwerpen hoger scoort dan de groepen die wel lid zijn van een belangenorganisatie. Het eerste onderwerp betreft 'meldingen bij het Cbp'. Indien geen sprake is van een lidmaatschap van een belangenorganisatie wordt in 82% van de gevallen vermeld dat de verwerking van persoonsgegevens is aangemeld bij het Cbp. Indien een online verzekeraar lid is van het Verbond van Verzekeraars, Thuiswinkel.org of van beide, zijn deze percentages respectievelijk 56%, 25% en 78%. Met betrekking tot het onderwerp 'het al dan niet verstrekken van persoonsgegevens aan derden' wordt in 75% hiervan melding gemaakt door online verzekeraars die geen lid zijn van een belangenorganisatie. Indien een online verzekeraar lid is van het Verbond van Verzekeraars, Thuiswinkel.org of van beide, zijn deze percentages respectievelijk 25%, 67% en 56%.

4.12.2 Lidmaatschap: Segment Reizen

Van de 100 online reiswinkels die zijn onderzocht (zie paragraaf 4.3) kan een deel zowel lid zijn van de ANVR, van Thuiswinkel.org alsook van beide belangenorganisaties.

Allereerst is onderzocht of er statistisch significante verschillen optreden ten aanzien van het gebruik van een privacyverklaring indien een online reiswinkel lid is van de ANVR. Voor de relevante kruistabellen die een onderling statistisch significant verschil laten zien wordt verwezen naar Bijlage E1.
Vervolgens is onderzocht of er statistisch significante verschillen optreden ten aanzien van het gebruik van een privacyverklaring indien een online reiswinkel lid is van Thuiswinkel.org. De hier relevante kruistabellen zijn opgenomen in Bijlage E2.

Uit het onderzoek kan worden geconcludeerd dat het niet veel uitmaakt of de online reiswinkel lid is van de ANVR: er zijn nauwelijks statistisch significante verschillen waar te nemen. Uit het onderzoek kan tevens worden afgeleid dat wel relevant is of de online reiswinkel lid is van Thuiswinkel.org: hier doen zich vrij veel statistisch significante verschillen voor.

Evenals bij de eerder besproken resultaten van online verzekeraars, kan ook hier de situatie zich voordoen dat de online reiswinkel zowel lid is van de ANVR als van Thuiswinkel.org. Ook hier is daarom onderzocht of er statistisch significante verschillen optreden indien de 100 online reiswinkels worden onderscheiden in 4 categorieën, te weten:

1. De online verzekeraar die noch lid is van de ANVR noch van Thuiswinkel.org.
2. De online verzekeraar die uitsluitend lid is van de ANVR.
3. De online verzekeraar die uitsluitend lid is van Thuiswinkel.org.
4. De online verzekeraar die zowel lid is van de ANVR als van Thuiswinkel.org.

Wederom moet worden aangetekend dat de onderverdeling in 4 categorieën tot gevolg heeft dat iedere groep, vanuit statistisch oogpunt bekeken, een beperkt aantal online reiswinkels omvat. Dit heeft tot gevolg dat resultaten weliswaar statistisch significante verschillen laten zien, maar vanwege de beperkte omvang slechts als indicatief kunnen worden beschouwd. Voor de relevante kruistabellen: zie Bijlage E3. Hieronder worden de resultaten besproken.

Aanwezigheid van een privacyverklaring

Indien een online reiswinkel geen lid is van een belangenorganisatie, blijkt in 64% van de gevallen een privacyverklaring op de website geplaatst. Indien een online reiswinkel lid is van Thuiswinkel.org bedraagt dit percentage 100%. In het geval dat de online reiswinkel zowel lid is van de ANVR als Thuiswinkel.org, is in 96% van de gevallen een privacyverklaring op de website opgenomen.

Identiteit

Kijkend naar de wijze waarop de identiteit kenbaar wordt gemaakt, dan blijkt dit veelal de handelsnaam te zijn, en niet de statutaire naam. De percentages met betrekking tot het laatst genoemde liggen tussen de 12% en 15%. Dit is anders indien de online reiswinkel lid is van de ANVR, in welk geval in 48% van de gevallen de statutaire naam wordt genoemd.

Recht op toegang en verzet

Indien een online reiswinkel geen lid is van een belangenorganisatie, blijkt in 38% te worden aangegeven dat de betrokkene recht heeft op toegang tot zijn persoonsgegevens. Indien de online reiswinkel lid is van Thuiswinkel.org bedraagt dit percentage 54%. In het geval dat de online reiswinkel zowel lid is van de ANVR als van Thuiswinkel.org, is de score met 68% het hoogst.

Indien een online reiswinkel geen lid is van een belangenorganisatie, wordt in 63% vermeld dat de betrokkene recht heeft op verzet tegen de verwerking van zijn persoonsgegevens. Indien de online reiswinkel lid is van Thuiswinkel.org bedraagt dit percentage 69%, en waar de online reiswinkel zowel lid is van de ANVR als van Thuiswinkel.org blijkt de score met 92% het hoogst.

Elektronische adres van de verantwoordelijke

In de gevallen dat de online reiswinkel geen lid is van een belangenorganisatie, blijkt in 38% van de gevallen het elektronische adres van de verantwoordelijke te worden aangegeven. Indien een online reiswinkel lid is van Thuiswinkel.org bedraagt dit percentage 77%. Bij een lidmaatschap van zowel de ANVR als van Thuiswinkel.org blijkt in 84% van de gevallen het elektronische adres van de verantwoordelijke te worden genoemd.

Beveiligingsmaatregelen

In de gevallen dat een online reiswinkel geen lid is van een belangenorganisatie, maakt 25% van de gevallen melding van het feit dat de verantwoordelijke beveiligingsmaatregelen heeft getroffen ter bescherming van de persoonsgegevens. Indien een online reiswinkel lid is van Thuiswinkel.org bedraagt dit percentage 62%. En bij het dubbele lidmaatschap (zowel ANVR als Thuiswinkel.org), maakt 60% melding van het nemen van beveiligingsmaatregelen.

4.12.2.1 Conclusie met betrekking tot het segment Reizen

Uit het voorgaande volgt dat, waar het gebruik van een privacyverklaring binnen het segment Reizen betreft, het lidmaatschap van een belangenorganisatie een relevante factor is. Dit geldt echter uitsluitend waar het een lidmaatschap van Thuiswinkel.org betreft. Opvallend genoeg blijkt het lidmaatschap van ANVR niet relevant te zijn.

4.12.3 Lidmaatschap: Segment Kleding

Kijken we naar de 100 onderzochte online kledingwinkels, dan kunnen deze zowel lid zijn van CBW-MITEX, van Thuiswinkel.org alsook van beide belangenorganisaties. Op grond van haar moverende redenen heeft CBW-MITEX geen specifieke lidmaatschapsgegevens willen verstrekken. Wel heeft CBW-MITEX laten weten dat van alle voor dit onderzoek geselecteerde online kledingwinkels er vrijwel geen lid zijn van haar organisatie. Het was aldus voor het onderhavige onderzoek niet mogelijk een onderscheid te maken tussen een al dan niet lidmaatschap van de organisatie CBW-MITEX en/of Thuiswinkel.org. De onderzochte websites zijn daarom als volgt onderscheiden:

1. De online kledingwinkel die geen lid is van Thuiswinkel.org.
2. De online kledingwinkel die lid is van Thuiswinkel.org.

Voor de relevante kruistabellen die ten aanzien van het segment Kleding een onderling statistisch significant verschil laten zien wordt verwezen naar Bijlage F.

Aanwezigheid privacyverklaring

In 63% van de gevallen waarin de online kledingwinkel geen lid is van Thuiswinkel.org, blijkt een privacyverklaring op de website geplaatst. Daar waar wel sprake is van het lidmaatschap bedraagt dit percentage 100%.

Mogelijkheid tot opslaan van de privacyverklaring

Bij 2% van de online kledingwinkels die geen lid is van Thuiswinkel.org kan de privacyverklaring worden opgeslagen. In geval van een lidmaatschap is dit percentage 27%.

Elektronische algemene voorwaarden

Van de online kledingwinkels die geen lid zijn van Thuiswinkel.org, blijkt 53% in de elektronische algemene voorwaarden bepalingen te hebben opgenomen die zien op de verwerking van persoonsgegevens. Bij de leden van Thuiswinkel.org is dit 23%.

Identiteit

Daar waar de online kledingwinkel lid is van Thuiswinkel.org worden in alle gevallen gegevens over de identiteit van de verantwoordelijke vermeld. Bij afwezigheid van het lidmaatschap is dit in 12% van de gevallen. Indien informatie over de identiteit wordt vermeld, blijkt in 45% te worden verwezen naar de statutaire naam als de online kledingwinkel lid is van Thuiswinkel.org. Indien de online kledingwinkel geen lid is van Thuiswinkel.org, is dit in 10% het geval.

Recht op toegang tot de persoonsgegevens

Indien een online kledingwinkel lid is van Thuiswinkel.org vermeldt 82% dat de betrokkene recht heeft op toegang tot zijn persoonsgegevens. Dit percentage daalt naar 47% wanneer men geen lid is van Thuiswinkel.org.

Fysiek en elektronisch adres van de verantwoordelijke

In 55% van de gevallen waarin de online kledingwinkel lid is van Thuiswinkel.org blijkt het fysieke adres van de verantwoordelijke te worden genoemd. Dit percentage bedraagt 20% bij afwezigheid van het lidmaatschap.

Kijken we naar de vermelding van het elektronisch adres, dan stellen we vast dat 73% van de online kledingwinkels die lid is van Thuiswinkel.org, het elektronisch adres van de verantwoordelijke noemt. Dit is 41% bij de niet-leden.

Gebruik van cookies

Van de kledingwinkels die lid zijn van Thuiswinkel.org, laat 91% weten of er al dan niet gebruik wordt gemaakt van cookies. Dit percentage bedraagt 55% onder de niet-leden.

Contactpersonen in verband met de uitoefening van rechten of het hebben van vragen

Net iets meer dan 40% (concreet 41%) van de niet-leden maakt melding van de naam van de afdeling tot wie de betrokkene zich moet wenden om zijn rechten uit te oefenen. Indien een online kledingwinkel wel lid is van Thuiswinkel.org, bedraagt dit percentage 68%.

Van de niet-leden vermeldt 35% de naam van de afdeling tot wie de betrokkene zich moet wenden in verband met vragen omtrent de verwerking van persoonsgegevens. Bij de leden ligt dit percentage op 73%.

Wijziging van de privacyverklaring

In de gevallen waarin de verantwoordelijke zich het recht voorbehoudt de inhoud van de privacyverklaring eenzijdig te wijzigen, informeert 64% de betrokkene hierover indien er sprake is van een lidmaatschap van Thuiswinkel.org. Is de verantwoordelijke geen lid van Thuiswinkel.org, dan wordt de betrokkene bij 21% van de websites geïnformeerd over de aanpassing van de privacyverklaring.

(Rechts)maatregelen

In het geval een online kledingwinkel lid is van Thuiswinkel.org, maakt 23% van deze online winkels melding van de (rechts)maatregelen die de betrokkene ter beschikking staan indien de verantwoordelijke tekortschiet in het naleven van de wet bij het verwerken van de persoonsgegevens of anderszins onrechtmatig handelt jegens de betrokkene. In de gevallen dat de online kledingwinkel geen lid is van Thuiswinkel.org, bedraagt dit percentage 6%.

4.12.3.1 Conclusie met betrekking tot het segment Kleding

Vatten we het voorgaande samen, dan kunnen we vaststellen dat het lidmaatschap van Thuiswinkel.org een relevante factor blijkt te zijn. Dit lidmaatschap leidt ten aanzien van het gebruik van een privacyverklaring tot een aanzienlijk aantal statistisch significante verschillen.

4.13 Systematische samenvatting en conclusies ten aanzien van het empirisch onderzoek

4.13.1 Systematische samenvatting

In de voorgaande paragrafen zijn de resultaten besproken die zijn verkregen uit het empirisch onderzoek onder in totaal 257 online websites in de segmenten Verzekeringen, Reizen en Kleding. Ter afronding zullen in het navolgende de relevante resultaten geabstraheerd van de specifieke branche worden weergegeven. Daarbij moet overigens wel worden aangetekend dat in 24% van de onderzochte gevallen geen privacyverklaring op de website was opgenomen. De hieronder gepresenteerde resultaten hebben daarom betrekking op de gevallen (n=196; 76%) waarin wel een privacyverklaring beschikbaar was.

Vorm en kenbaarheid van privacyverklaring

- In 92% van de gevallen wordt de privacyverklaring verstrekt aan de hand van een hyperlink.
- In 99% wordt de privacyverklaring niet in een getrapte vorm gepresenteerd.
- In 44% van de gevallen is ‘privacy’ de benaming van de button van de hyperlink of pop up scherm, en hanteert 19% de naam ‘privacystatement’.
- In 24% is de button van de hyperlink niet op de homepagina geplaatst.

- In 72% van de gevallen staat de button van de hyperlink onderaan de homepagina.
- In 92% dient de betrokkene te scrollen voordat de button van de hyperlink op de homepagina zichtbaar wordt.
- In 91% van de gevallen wordt de betrokkene niet de mogelijkheid geboden de privacyverklaring op te slaan.

Inhoud: verplichte elementen identiteit van de verantwoordelijke en doel van de verwerking op grond van artikel 33 en 34 Wbp

- In 4,1% van de gevallen wordt in de privacyverklaring geen melding gemaakt van de identiteit van de verantwoordelijke.
- In 63% wordt in de privacyverklaring de handelsnaam genoemd. In geen van de gevallen wordt de naam van de natuurlijke persoon genoemd indien de online winkel een eenmanszaak betreft. De statutaire naam ontbreekt in 33% van de gevallen.
- In 90% van de gevallen wordt het doel van de verwerking genoemd.

Inhoud: recht op toegang, rectificatie, verwijderen en verzet (passieve informatieplicht):

- Van het recht van de betrokkenen op toegang tot de persoonsgegevens maakt 44% geen melding.
- In 48% van de gevallen wordt geen melding gemaakt van het recht van de betrokkene op rectificatie van zijn persoonsgegevens.
- In 74% van de gevallen wordt geen melding gemaakt van het recht van de betrokkene op verwijdering van de persoonsgegevens.
- In 24% van de gevallen wordt geen melding gemaakt van het recht van de betrokkene om zich, afhankelijk van de situatie, te verzetten tegen de verwerking van persoonsgegevens.

Inhoud: het doel van de privacyverklaring

- In alle gevallen wordt in de privacyverklaring niet vermeld dat de verantwoordelijke aan de hand van de privacyverklaring wil voldoen aan zijn informatieplicht die hij heeft op grond van de Wbp.

Inhoud: fysieke en elektronische adres van de verantwoordelijke

- In 79% van alle gevallen wordt het fysieke adres van de verantwoordelijke niet vermeld.
- In 54% van alle gevallen wordt het elektronische adres van de verantwoordelijke niet vermeld.

Inhoud: verwerking van bijzondere gegevens

- In 80% van alle gevallen wordt niet vermeld of verduidelijkt dat er bijzondere gegevens worden verwerkt.

Inhoud: verplichte of facultatieve verstrekking van gegevens

- In 96% van alle gevallen wordt niet vermeld of het verstrekken van bepaalde informatie verplicht of facultatief is.

Inhoud: categorieën van ontvangers

- In 84% van alle gevallen wordt niet vermeld voor welke (categorieën van) ontvangers binnen de organisatie van de verantwoordelijke de verzamelde persoonsgegevens bestemd zijn.

Inhoud: bewaartermijnen

- In 93% van alle gevallen wordt niet vermeld hoe lang de bewaartermijn van de verzamelde persoonsgegevens is.

Inhoud: gebruik van cookies

- In 30% van alle gevallen wordt geen melding gemaakt dat de website al dan niet gebruik maakt van cookies.

Inhoud: beveiligingsmaatregelen

- In 46% van alle gevallen wordt niet vermeld of er beveiligingsmaatregelen zijn getroffen om bijvoorbeeld de authenticiteit, integriteit en vertrouwelijkheid van de persoonsgegevens te waarborgen.

Inhoud: melding bij het College bescherming persoonsgegevens

- In 64% van alle gevallen wordt niet vermeld dat een verwerking is aangemeld bij het College bescherming persoonsgegevens.

Inhoud: contactpersoon van de verantwoordelijke

- In 61% van alle gevallen wordt geen melding gemaakt van de naam en het adres tot wie de betrokkene zich moet wenden om zijn rechten uit te oefenen.
- In 63% van alle gevallen wordt niet de naam van de afdeling of functionaris vermeld die verantwoordelijk is voor het beantwoorden van vragen betreffende de verwerking van persoonsgegevens.

Inhoud: verstrekking van persoonsgegevens aan derden

- In 20% van alle gevallen wordt niet vermeld of persoonsgegevens al dan niet aan derden worden verstrekt.
- In 52% van alle gevallen worden er geen derden benoemd.
- In 96% van de gevallen wordt niet vermeld dat persoonsgegevens, al dan niet mogelijk, aan derden in het buitenland worden verstrekt.

- In 85% van alle gevallen wordt niet vermeld dat derden de vertrouwelijkheid en/of beveiliging van de persoonsgegevens garanderen.

Inhoud: rechtsmaatregelen

- In 87% van alle gevallen wordt geen melding gemaakt welke rechtsmaatregelen de betrokkene kan treffen indien de verantwoordelijke tekortschiet in het verwerken van de persoonsgegevens of onrechtmatig handelt jegens de betrokkene.

Inhoud: wijziging van de privacyverklaring

- In 48% van alle gevallen behoudt de verantwoordelijke zich het recht voor om de inhoud van de privacyverklaring eenzijdig te wijzigen.
- In die gevallen dat de verantwoordelijke zich het recht voorbehoudt om de inhoud van de privacyverklaring eenzijdig te wijzigen, dient in 71% van alle gevallen de betrokkene zelf de privacyverklaring op de website regelmatig te raadplegen om te kunnen beoordelen of er wijzigingen hebben plaatsgevonden.

Privacyverklaring en elektronische algemene voorwaarden

- Indien de verantwoordelijke een privacyverklaring heeft, alsmede elektronische algemene voorwaarden, dan zijn in 24% van de gevallen ook materiële bepalingen opgenomen in die elektronische algemene voorwaarden met betrekking tot de verwerking van persoonsgegevens.

4.13.2 Conclusies met betrekking tot verschillen tussen de segmenten Verzekeringen, Reizen en Kleding

Om een beeld te krijgen van de verhoudingen tussen de segmenten Verzekeringen, Reizen en Kleding, zijn de statistisch significante resultaten geïnventariseerd en geselecteerd. Vervolgens zijn aan deze resultaten per segment een waarde toegekend van een 3, 2 of 1 (het segment met de hoogste percentuele score krijgt de waarde 3 toegekend).

Aanwezigheid, vorm en kenbaarheid van de privacyverklaring

Kijken we naar de enkele vermelding op een website van een privacyverklaring, dan stellen we vast dat het segment Verzekeringen hier het hoogst scoort. De percentages voor de segmenten Reizen en Kleding zijn hier gelijk. Het segment Verzekeringen scoort het hoogst als het gaat om het plaatsen van een hyperlink op de homepagina, gevolgd door het segment Kleding en Reizen. Dit leidt ertoe dat het segment Verzekeringen de hoogste totaalscore (waarde 6) heeft waar het gaat om de aanwezigheid, vorm en kenbaarheid van de privacyverklaring, gevolgd door het segment Kleding (waarde 4) en Reizen (waarde 3).

Tabel 4.53 Kenbaarheid en vorm van de privacyverklaring	Score Verzekeringen		Score Reizen		Score Kleding	
	%	score	%	score	%	score
De winkel heeft een online privacyverklaring op zijn website	94,7	3	71,0	2	71,0	2
De button van de hyperlink staat op de homepagina	92,2	3	65,1	1	74,6	2
Totaalscore per segment		6		3		4

Inhoud van de privacyverklaring: verplichte elementen

De score voor verstrekte informatie over de identiteit is het hoogst voor het segment Reizen, gevolgd door het segment Verzekeringen en het segment Kleding. Het segment Verzekeringen scoort het hoogst wat betreft het vermelden van het doel van de verwerking. Hier volgen na het segment Verzekeringen het segment Kleding respectievelijk Reizen. Het voorgaande resulteert voor het segment Verzekeringen in de hoogste totaalscore, namelijk de waarde 5, waar het gaat om het vermelden van de verplichte elementen identiteit en doel van de verwerking. De waarden van de segmenten Reizen en Kleding zijn respectievelijk 4 en 3.

Tabel 4.54 Inhoud van de privacyverklaring: verplichte elementen	Score Verzekeringen		Score Reizen		Score Kleding	
	%	score	%	score	%	score
De identiteit van de verantwoordelijke wordt vermeld	98,1	2	98,6	3	91,5	1
Het doel van de verwerking wordt vermeld	98,1	3	84,5	1	90,1	2
Totaalscore per segment		5		4		3

Inhoud van de privacyverklaring: passieve informatieplicht

Met betrekking tot de passieve informatieplicht behaalt het segment Verzekeringen de hoogste waarde (11), gevolgd door het segment Kleding (9) en het segment Reizen (4).

Tabel 4.55 Inhoud van de privacyverklaring: passieve informatieplicht	Score Verzekeringen		Score Reizen		Score Kleding	
	%	score	%	score	%	score
Er wordt melding gemaakt van het recht op toegang tot de persoonsgegevens	72,2	3	40,8	1	57,7	2
Er wordt melding gemaakt van het recht om zich te verzetten tegen een verwerking	75,9	2	70,4	1	80,3	3
Er wordt melding gemaakt van het recht op rectificatie van de gegevens	64,8	3	32,4	1	62,0	2
Er wordt melding gemaakt van het recht op verwijdering van de gegevens	37,0	3	16,9	1	26,8	2
Totaalscore per segment		11		4		9

Inhoud: nadere informatie

De nadere informatie die door de verantwoordelijke dient te worden verstrekt opdat een behoorlijke en zorgvuldige verwerking wordt gewaarborgd, kan bestaan uit diverse elementen. Als we kijken naar nader verstrekte informatie scoort het segment Verzekeringen met een waarde van 39 het hoogst, gevolgd door het segment Kleding (waarde 34) en het segment Reizen (waarde 26).

Tabel 4.56 Inhoud van de privacyverklaring: overige nadere informatie	Score Verzekeringen		Score Reizen		Score Kleding	
	%	score	%	score	%	score
Het privacybelang van de betrokkene wordt erkend	78,9	3	78,9	3	52,1	2
Het fysieke adres van de verantwoordelijke wordt vermeld	14,8	1	15,5	2	31,0	3
Het elektronische adres van de verantwoordelijke wordt vermeld	27,8	1	56,3	3	50,7	2
Er wordt vermeld dat de verwerking is aangemeld bij het Cbp	61,1	3	38,0	2	14,1	1

Er wordt vermeld dat er bijzondere gegevens worden verwerkt	68,5	3	0,0	1	2,8	2
Er wordt vermeld voor welke (categorieën) ontvangers de persoonsgegevens bestemd is/zijn.	48,1	3	0,0	2	0,0	2
Er wordt vermeld of het verstrekken van gegevens van bepaalde informatie verplicht of facultatief is	0,0	1	2,8	2	8,5	3
Er wordt vermeld dat er beveiligingsmaatregelen zijn getroffen	70,4	3	42,3	1	52,1	2
Er wordt vermeld dat persoonsgegevens aan derden worden verstrekt	55,6	1	88,7	2	90,1	3
Er worden derden benoemd	66,7	3	31,0	1	50,7	2
Er wordt vermeld dat derden de vertrouwelijkheid en/of beveiliging van de persoonsgegevens garanderen	16,7	2	2,8	1	25,4	3
Er wordt melding gemaakt van de naam/functie/afdeling tot wie de betrokkene zich kan wenden indien hij zijn rechten wil uitoefenen	55,6	3	15,5	1	49,3	2
Er wordt melding gemaakt van de naam/functie/afdeling tot wie de betrokkene zich kan wenden indien hij vragen heeft over de verwerking	53,7	3	15,5	1	46,5	2
Er wordt melding gemaakt welke (rechts)maatregelen de betrokkene kan treffen indien de verantwoordelijke in strijd handelt met de Wbp of privacyverklaring	29,6	3	1,4	1	11,3	2

Er wordt vermeld dat de persoonsgegevens, al dan niet mogelijk, naar een derde in het buitenland worden verstrekt.	5,6	3	4,2	2	2,8	1
Er wordt vermeld dat de betrokkene, al dan niet voor specifieke verwerkingen, toestemming moet geven of heeft gegeven aan de verantwoordelijke om zijn persoonsgegevens te mogen verwerken.	38,9	3	15,5	1	25,4	2
Totaalscore per segment		39		26		34

4.13.3 Conclusie

In het licht van het voorgaande kan worden geconcludeerd dat waar het gebruik van een privacyverklaring betreft, het segment Verzekeringen met een totale waarde van 61 het hoogst scoort, gevolgd door het segment Kleding met een waarde van 50, gevolgd door het segment Reizen met een waarde van 37.

Tabel 4.57 Totale score per segment	Score Verzekeringen	Score Reizen	Score Kleding
Kenbaarheid en vorm van de privacyverklaring	6	3	4
Inhoud van de privacyverklaring: verplichte elementen	5	4	3
Inhoud van de privacyverklaring: passieve informatieplicht	11	4	9
Inhoud van de privacyverklaring: overige nadere informatie	39	26	34
Totaal score per segment	**61**	**37**	**50**

Het lag in de lijn der verwachting dat de analyse bij het segment Verzekeringen in de hoogste totaalwaarde zou resulteren. Immers, binnen dit segment worden persoonsgegevens verwerkt die, ten opzichte van de andere segmenten, de hoogste mate van gevoeligheid hebben.[434] Voorts is dit segment het meest georganiseerd en gereguleerd ten opzichte van de andere segmenten.[435] Dit uit zich onder meer in een verplichting van de

[434] Zie paragraaf 4.2.2.

[435] Zie paragraaf 4.2.3.

leden van de belangenorganisatie Verbond van Verzekeraars om een privacyverklaring op de website te plaatsen.

Kijkend naar het type persoonsgegevens dat wordt verwerkt, valt op dat het segment Reizen een lagere totaalscore heeft dan het segment Kleding. De persoonsgegevens die in het segment Reizen worden verwerkt omvatten immers onder meer gegevens van identiteitsbewijzen, budgetten en een eventueel strafrechtelijk verleden. Het type gegevens dat wordt verwerkt binnen het segment Kleding is naar verwachting relatief het minst 'gevoelig'.[436] Duidelijk is in ieder geval dat het segment Reizen een hogere mate van georganiseerdheid en gereguleerdheid kent ten opzichte van het segment Kleding. Dit uit zich onder meer in een verplichting van de leden van de belangenorganisatie ANVR om zich te conformeren aan de Internetgedragscode, waarin onder meer is opgenomen dat de leden de plicht hebben om persoonsgegevens te verwerken conform de Wbp (artikel 6 sub a. Internetgedragscode ANVR). Uit het empirisch onderzoek kan echter worden geconcludeerd dat het niet veel uitmaakt of de online reiswinkel lid is van de ANVR. Dit zou kunnen betekenen dat het opleggen van een 'algemene verplichting' via een gedragscode om 'persoonsgegevens te verwerken conform de Wbp' geen noemenswaardig effect heeft op het gebruik van een privacyverklaring. De analyses laten zien dat een verplicht gebruik van een privacyverklaring, zoals opgelegd door de belangenorganisaties Verbond van Verzekeraars en Thuiswinkel.org, wel een effect heeft.[437]

[436] Om te spreken in de woorden van Van Esch & Blok. Van Esch & Blok, p. 220.

[437] Zie paragraaf 4.12.1.1, 4.12.2.1 en 4.12.3.1.

Hoofdstuk 5 | De privacyverklaring in het licht van transparantie en accountability

5.1 Inleiding

In dit hoofdstuk wordt in paragraaf 5.2 teruggeblikt op de conclusies uit de voorgaande hoofdstukken. Op basis van de observaties zullen knelpunten worden gesignaleerd ten aanzien van het gebruik van privacyverklaringen. Het kabinet en diverse instanties benadrukken het belang van transparantie in relatie tot het verwerken van persoonsgegevens. In paragraaf 5.3 wordt daarom ingegaan op nadere sturingsmogelijkheden voor de toepassing en inhoudelijke invulling van de privacyverklaring ten behoeve van transparantie. Naar aanleiding van eerder onderzoek naar het gebruik van privacyverklaringen in de Verenigde Staten, wordt aldaar momenteel ingezet op het ontwikkelen van gestandaardiseerde privacyverklaringen. Paragraaf 5.4 benoemt een aantal initiatieven dat daaromtrent in de Verenigde Staten is geïnitieerd. In paragraaf 5.5 zal het thema accountability aan de orde komen, en wordt bezien in hoeverre een privacyverklaring daadwerkelijk betekenis kan krijgen voor accountability. Dit hoofdstuk wordt in paragraaf 5.6 afgesloten met conclusies.

5.2 Knelpunten en discussie met betrekking tot het gebruik van de privacyverklaring

Centraal in hoofdstuk 2 stond de informatieplicht die de verantwoordelijke op grond van de Wbp in acht dient te nemen jegens de betrokkene. In het bijzonder zijn in dat verband de artikelen 33 en 34 Wbp relevant. De verantwoordelijke dient op grond van deze artikelen de betrokkene te informeren over zijn identiteit alsmede over het doel waarvoor de persoonsgegevens worden verwerkt. Bovendien dient de verantwoordelijke nadere informatie aan de betrokkene te verstrekken ter waarborging van een behoorlijke en zorgvuldige verwerking. Dit hoeft hij echter alleen te doen indien en voor zover dat nodig is gelet op (i) de aard van de gegevens en/of (ii) de omstandigheden waaronder de gegevens worden verkregen en/of (iii) het gebruik dat van de gegevens wordt gemaakt. Waar het meer concreet over de privacyverklaring gaat, legt de Wbp geen verplichtingen op wat betreft vorm en wijze waarop deze verklaring kenbaar dient te worden gemaakt.

Uit het empirisch onderzoek onder 257 online winkels blijkt dat in 76% van de gevallen de verantwoordelijke een privacyverklaring op zijn website heeft geplaatst. Tevens wordt duidelijk dat 92% van de verantwoordelijken de privacyverklaring aanbiedt via een hyperlink. Het gebruik van deze wijze van aanbieden geniet niet de voorkeur van de Groep Gegevensbescherming Artikel 29. Deze is van mening dat de informatie aan de betrokkene

rechtstreeks op het scherm dient te worden gepresenteerd, zonder dat de betrokkene zelf actie hoeft te ondernemen om toegang te krijgen tot de via de privacyverklaring aangeboden informatie. De Groep Gegevensbescherming Artikel 29 geeft daarom de voorkeur aan het presenteren van de informatie aan de hand van tekstvensters op het moment dat de persoonsgegevens worden verzameld. Tevens opteert de Groep voor een getrapte verstrekking van informatie in maximaal 3 treden. Ook in dit opzicht wordt, zoals uit het empirisch onderzoek blijkt, het advies van de Groep Gegevensbescherming Artikel 29 niet gevolgd. Immers, in 99% van de gevallen wordt de privacyverklaring niet in een getrapte vorm aangeboden. De button van de privacyverklaring is veelal niet in een oogopslag zichtbaar. In 92% van alle gevallen dient de betrokkene te scrollen voordat de 'hyperlinkbutton' van de privacyverklaring op de homepagina zichtbaar wordt. Bovendien plaatst 72% van de verantwoordelijken de button van de privacyverklaring onderaan de homepagina.

In de empirie is wat betreft de inhoud van de privacyverklaringen een grote variëteit aangetroffen. Zo worden zeer uitgebreide privacyverklaringen gehanteerd, maar ook privacyverklaringen die slechts enkele regels omvatten. Met betrekking tot de identiteit van de verantwoordelijke maakt 4,1% hiervan geen melding in de privacyverklaring, terwijl in 63% van alle gevallen de handelsnaam van de verantwoordelijke kenbaar wordt gemaakt. Dit is niet conform de vereisten van de Wbp, aangezien in geval van een eenmanszaak de naam van de natuurlijke persoon genoemd dient te worden, en in geval van een besloten of naamloze vennootschap de statutaire naam van die vennootschap. Tegelijkertijd voldoet van alle privacyverklaringen 90% aan de verplichting om het doel van verwerking kenbaar te maken. In hoofdstuk 2 is gerefereerd aan de 'passieve' informatieplicht zoals die volgt uit artikel 35 Wbp en artikel 41 Wbp. Op grond van artikel 35 lid 1 Wbp heeft de betrokkene het recht om zich te wenden tot de verantwoordelijke met het verzoek hem mede te delen of persoonsgegevens van hem worden verwerkt. De verantwoordelijke heeft op grond van hetzelfde lid de plicht om de betrokkene binnen vier weken schriftelijk te informeren of hem betreffende persoonsgegevens worden verwerkt. Uit het empirisch onderzoek volgt dat in 44% van alle gevallen geen melding wordt gemaakt van het recht van de betrokkene op toegang tot zijn persoonsgegevens. Ook heeft de verantwoordelijke op grond van artikel 41 lid 3 Wbp de plicht om de betrokkene te informeren dat hij zich kan verzetten tegen het voornemen van de verantwoordelijke om persoonsgegevens aan derden te verstrekken of voor rekening van derden te gebruiken met het oog op werving voor commerciële of charitatieve doelen. Uit het empirisch onderzoek volgt dat 24% van de verantwoordelijken geen melding maakt van het recht van de betrokkene om zich, afhankelijk van de situatie, te verzetten tegen de verwerking van zijn persoonsgegevens.
Verder toont het empirisch onderzoek een afwijkend beeld ten opzichte van de theoretische observaties uit hoofdstuk 2. Zo laat de praktijk zien dat de elementen zoals genoemd in tabel 2.5 veelal niet of niet volledig in de privacyverklaring worden opgenomen. Tevens

tonen de resultaten uit het empirisch onderzoek een ander beeld dan hetgeen wordt geambieerd in de MvT, waar wordt opgemerkt dat informatie gemakkelijk te vinden moet zijn en opgesteld in begrijpelijke bewoordingen. “Een onopvallende link naar deze informatie in een klein lettertype onderaan de site (onder de ‘vouw’ van de site waarvoor de gebruiker eerst naar beneden moet scrollen) zal dus niet voldoende zijn om aan deze informatieplicht te voldoen”.[438] Verder is relevant dat Zwenne et al. concluderen dat de open normen uit de artikelen 33 en 34 Wbp leiden tot interpretatiemoeilijkheden. Het beeld dat volgt uit het empirisch onderzoek lijkt deze conclusie te bevestigen, gezien de diversiteit in inhoud van de onderzochte privacyverklaringen.

Uit hoofdstuk 3 volgt onder meer dat het voor de betrokkene complex is om te bepalen welke (juridische) maatregelen hij op grond van het BW kan treffen indien de verantwoordelijke zijn verplichtingen uit hoofde van de privacyverklaring niet nakomt. Uit het empirisch onderzoek blijkt dat in de privacyverklaring deze (juridische) maatregelen niet aan de betrokkene worden uitgelegd of verduidelijkt. Tevens blijkt dat in de privacyverklaring niet, of nagenoeg niet, wordt uiteengezet of de privacyverklaring dient te worden opgevat als een aanbod van de verantwoordelijke, en de verklaring de status van overeenkomst krijgt na aanvaarding door de betrokkene. Voorts volgt uit het empirisch onderzoek dat er niet of nauwelijks wordt gerefereerd aan verwerkingen op basis van toestemming, ondubbelzinnige of uitdrukkelijke toestemming van de betrokkene.

In het licht van het voorgaande kan worden geconcludeerd dat de aanbevelingen van de Groep Gegevensbescherming Artikel 29 in de praktijk in vele opzichten niet worden opgevolgd. Een reden daarvoor zou kunnen zijn dat de adviezen niet bindend voor de verantwoordelijke zijn. Tevens is het niet duidelijk of de elementen die zijn opgenomen in de eerder in dit onderzoek gepresenteerde tabel 2.5 op grond van de Wbp verplicht moeten worden genoemd in de privacyverklaring. Daarbij is het de vraag of de verantwoordelijke weet heeft van het bestaan van de adviezen van de Groep Gegevensbescherming Artikel 29 of die van het Cbp. Eerder volgde uit het onderzoek van Zwenne et al. dat de informatieplicht uit de Wbp bij weinig verantwoordelijken bekend is. Het is voorstelbaar dat, nu de informatieplicht niet of onvoldoende bekend is, de verantwoordelijke ook geen weet heeft van de wijze waarop hij met behulp van een privacyverklaring invulling kan geven aan die informatieplicht. In dat kader is het niet ondenkbaar dat de verantwoordelijke die wel een privacyverklaring op zijn website heeft opgenomen dit primair heeft gedaan omdat andere online winkels ook een privacyverklaring hebben geplaatst, zonder zich daarbij af te vragen dan wel te beseffen op welke grond hij daartoe verplicht is. Een mogelijke aanwijzing

[438] Kamerstukken II 2010-2011, 32549, nr. 3, p. 80. Voor de volledigheid dient te worden opgemerkt dat de MvT deze opmerking plaatst in het kader van het gebruik van cookies. In hoofdstuk 2 werd echter duidelijk dat de informatieplicht uit de Wbp ook geldt ten aanzien van het gebruik van cookies.

hiervoor is gelegen in het feit dat, zoals volgt uit het empirisch onderzoek, in geen van de privacyverklaringen melding wordt gemaakt dat de verantwoordelijke met behulp van de privacyverklaring wil voldoen aan zijn informatieplicht.

Het algehele beeld dat uit het empirisch onderzoek naar voren komt lijkt overeen te stemmen met eerder, overigens deels in aantallen websites beperkt, uitgevoerd onderzoek naar het gebruik van privacyverklaringen in Nederland. In 2006 heeft Dubbeld onderzoek gedaan naar het privacybeleid van zes Nederlandstalige websites, zes websites van Amerikaanse bedrijven, en zes bedrijven met hoofdvestigingen in andere landen (twee in Duitsland, en verder in Frankrijk, Italië, Zwitserland en Israël). Alle websites betroffen telemedicine websites.[439] Uit haar onderzoek volgt onder meer dat vier van de zes Nederlands websites privacystatements bevatten.[440] Dubbeld concludeert dat de grote meerderheid van de onderzochte websites niet voldoet aan de eisen die worden gesteld aan privacystatements.[441] In 2009 presenteerden Beldad et al. de resultaten van onderzoek naar het gebruik van privacyverklaringen onder 100 gemeentelijke websites. Van dit aantal had 77% een privacyverklaring. “Only 77% (n=77) of the 100 selected Dutch municipal websites contained privacy statements”.[442] In het onderhavige onderzoek onder online verzekeraars, reis- en kledingwinkels ligt het algehele percentage op 76% (76,3%). Het percentage per individuele sector bedraagt respectievelijk 95%, 71% en 71%. Met betrekking tot de plaatsing van privacyverklaringen op websites concluderen Beldad et al.: “In terms of the fundability of the privacy statements on the websites, only 23% (n=18) of the 77 municipal websites provided a conspicuous link (labeled as ‘privacy’ and displayed both on the lower section of the homepage and on succeeding pages) to the privacy statements, while 77% (n=59) of the privacy statements can be found in other links within the websites (e.g. proclaimed/disclaimer, colophon, about the site, or contact)”.[443] “The figures indicate a very high difficulty rating for finding a privacy statement since users may end up having to try a lot of links before they can actually locate and read the privacy statement of the municipal website, unless they know exactly that the said statement is located, for instance, in the disclaimer”.[444] Specifiek ten aanzien van de inhoud van de verklaringen namen Beldad et al. een grote verscheidenheid waar. “While some privacy statements are considerably long to the point of including all possible guarantees that are in accordance with the Personal Data Protection Act of the Netherlands; other privacy statements are relatively short, with only one or two sentences”.[445]

---

439 Dubbeld.
440 Dubbeld, p. 133.
441 Dubbeld, p. 135.
442 Beldad et al., p.564.
443 Beldad et al., p.564.
444 Beldad et al., p.564.
445 Beldad et al., p.565.

De discussie die thans voorligt is of de voorgaande observaties aanleiding geven het gebruik van de privacyverklaring anders te benaderen, bijvoorbeeld door meer op het gebruik van dit instrument en de inhoud daarvan te sturen. Kijkend naar de privacyverklaring is de ratio gelegen in het vorm en inhoud geven van de informatieplicht. In hoofdstuk 2 is besproken dat de informatieplicht zoals neergelegd in de artikelen 33 en 34 Wbp niet meer afdoende is gezien de huidige maatschappelijke en technologische ontwikkelingen. Recente opvattingen van diverse actoren, zoals de Europese Commissie, de Groep Gegevensbescherming Artikel 29 en overige adviescommissies, benadrukken de noodzaak van meer transparantie. In hoofdstuk 2 werd gerefereerd aan de conclusies van de Europese Commissie die van mening is dat transparantie een basisvoorwaarde is, willen individuen controle kunnen uitoefenen over hun eigen gegevens en zich van een effectieve bescherming van hun persoonsgegevens kunnen verzekeren. “Het is van wezenlijk belang dat individuen door degenen die voor de verwerking verantwoordelijk zijn goed en duidelijk, op een transparante wijze, worden geïnformeerd over hoe en door wie hun gegevens worden verzameld en verwerkt, voor welke doeleinden, gedurende welke periode en in hoeverre zij het recht hebben hun gegevens in te zien, te corrigeren of te wissen”.[446] Ook in de literatuur is veelvuldig het belang van transparantie benadrukt. Zo stellen Bigo et al.: “The principles of transparency and openness are particularly important in the data protection field. Processing operations do not take place in public; neither are their results felt immediately by the individuals concerned, in order for them to respond accordingly. On the contrary, the processing of personal data takes place behind closed doors or rather within automated systems, without the millions of individuals whose data are being processed being present or even aware that such processing takes place. In addition, the results of such processing in the majority of cases do not lead to direct action, positive or negative, for the individuals concerned, but are stored in computer systems for future use. These circumstances, especially when it comes to security-related processing, may at the least lead to frustration or even unlawful infringement of individual rights. In the real world, individuals may come across a decision that affects them (for instance, being unable to enter a country applying border controls) and be unaware of the findings from processing operations that have been used to formulate such a decision”.[447]
Ook de analyse in hoofdstuk 3 maakt duidelijk dat transparantie van belang is, onder meer omdat het een vereiste is als betrokkenen rechtsgeldig hun ondubbelzinnige toestemming willen verstrekken conform artikel 8 sub a Wbp. Maar ook in het kader van een juridisch onaantastbare aanvaarding van de privacyovereenkomst is de mate waarin transparantie richting de betrokkene wordt betracht een relevante factor.

446 COM (2010) 609 definitief, p. 6 e.v.
447 Bigo et al., p. 109.

In het vervolg van dit hoofdstuk zal daarom worden ingegaan op nadere sturingsmogelijkheden voor de toepassing en inhoudelijke invulling van de privacyverklaring ten behoeve van transparantie.

5.3 Transparantie in relatie tot de privacyverklaring

Diverse instanties hebben gewezen op de rol van privacyverklaringen bij het realiseren van transparantie. Het Cbp merkt op dat een actievere invulling van de transparantieverplichting gerealiseerd kan worden met behulp van privacystatements.[448] De Europese Commissie expliciteert in een mededeling uit 2010 dat transparantie in essentie vereist dat informatie vlot toegankelijk en gemakkelijk te begrijpen is, en dat eenvoudige taal wordt gebruikt. Daarbij tekent zij aan dat dit bijzonder relevant is in een online omgeving waarin privacyverklaringen vaak onduidelijk, moeilijk te vinden, ondoorzichtig en niet steeds conform de bestaande voorschriften zijn.[449] De Commissie overweegt derhalve een of meer standaard privacyverklaringen op te stellen die door de verantwoordelijken moeten worden gebruikt: "De Commissie zal overwegen een of meer EU-standaardformulieren ('privacyverklaringen') op te stellen die door de voor de verwerking van gegevens verantwoordelijken moeten worden gebruikt".[450] Uit het voorstel van de Europese Commissie (2012) lijkt te kunnen worden opgemaakt dat de Commissie dit voornemen zal doorzetten.[451]

> Article 11 Transparent information and communication
> 1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.
>
> Article 14 Information to the data subject
> 8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Het kabinet Rutte stelt in aansluiting dat een EU-brede standaardverklaring zinvol kan zijn.[452] De lijn die de Europese Commissie klaarblijkelijk voor ogen heeft is 'transparantie'

448 Cbp, Jaarverslag 2009, p. 49.
449 COM (2010) 609 definitief, p. 6 e.v.
450 COM (2010) 609 definitief, p. 7.
451 COM (2012) 11 final.
452 Kamerstukken II 2010-2011, 22122, nr. 1116, p. 4.

door ‘standaardisatie’. Standaardisatie zou moeten voorkomen dat er verschillen optreden ten aanzien van het gebruik van privacyverklaringen. “Differences in the contents of privacy statements suggest differences in organizational practices that are adopted to ensure that the privacy of clients' data is maintained. These differences in contents also reflect differences in interpretations, on the part of organizations, of what users are expecting to read in privacy statements”.[453] Het voordeel van standaardisatie kan zijn dat de betrokkene slechts een beperkt aantal modellen van privacyverklaringen tot zich hoeft te nemen.[454] Naar de mening van de Amerikaan Anthony, Commissioner van de Federal Trade Commission, is het voordeel van gestandaardiseerde privacyverklaringen dat consumenten zich snel kunnen vergewissen op welke wijze een organisatie omgaat met de verwerking en bescherming van persoonsgegevens, en of zij vervolgens met die organisatie zaken willen doen. “If privacy policies were presented in a standard format, a consumer could more readily ascertain whether an entity's information sharing practices sufficiently safeguard private information and consequently whether the consumer wishes to do business with the company”.[455]

Kijkend naar de conclusies in de eerdere hoofdstukken dienen naar mijn mening – redenerend vanuit transparantie – ten aanzien van privacyverklaringen de navolgende aspecten overwogen te worden:

1. De aanwezigheid van de privacyverklaring;
2. De naamgeving, traceerbaarheid en de toegankelijkheid van de privacyverklaring;
3. De vorm van de privacyverklaring; en
4. De inhoud, leesbaarheid en begrijpelijkheid van de privacyverklaring.

Deze aspecten zullen in de volgende paragrafen worden behandeld. In paragraaf 5.2 kwam aan de orde dat er in Nederland beperkt onderzoek heeft plaatsgevonden naar het gebruik van privacyverklaringen. Daarentegen is en wordt in de Verenigde Staten veel onderzoek gedaan naar het gebruik van privacyverklaringen. Alhoewel het gebruik van privacyverklaringen in de Verenigde Staten niet kan worden vergeleken met de toepassing daarvan in Nederland, kan dit onderzoek uit de Verenigde Staten wel als inspiratie dienen bij het denken over de wenselijke vorm en inhoud van de privacyverklaring. In het onderstaande wordt daarom bij de bespreking van de vier genoemde aspecten waar vermeldenswaard gewezen op de observaties en conclusies uit deze onderzoeken.

5.3.1 De aanwezigheid van de privacyverklaring

De aanwezigheid van een privacyverklaring is van belang omdat het veelal de enige informatiebron op de website is met betrekking tot de verwerking en bescherming van

[453] Beldad et al., p. 565.
[454] Oussayef, p. 129.
[455] Anthony.

persoonsgegevens.[456] Over de feitelijke kwaliteit van de gegevensbescherming is daarmee overigens nog niets gezegd. Naar de mening van Dubbeld wekken websites die weinig aandacht besteden aan privacy met de opname van een privacyverklaring de suggestie dat er in het geheel geen problemen bestaan met betrekking tot de bescherming van persoonsgegevens. “Misschien is het de inzet van dit soort websites om als het ware geen slapende honden wakker te maken, en het vertrouwen uit te stralen dat eventuele risico’s als een vanzelfsprekendheid en zonder ruchtbaarheid aan de orde zijn gesteld”.[457] Met andere woorden, de beschikbaarheid op de website van een privacyverklaring betekent nog geenszins dat er voor de betrokkene een transparante situatie wordt gecreëerd. Zo zal – zoals in de navolgende paragrafen nader wordt besproken - de betrokkene ook daadwerkelijk kennis van de inhoud van de privacyverklaring moeten nemen en de geboden informatie moeten kunnen begrijpen. “Users must, if they are serious about protecting their privacy, check the privacy policy of every site they visit, and in most cases check it again every time they visit the site”.[458] Uit onderzoek in Nederland blijkt dat betrokkenen meer bereid zijn persoonsgegevens te verstrekken indien er een privacyverklaring op de website is geplaatst. “Over half of the total number of respondents in this study indicated that a privacy statement on a municipal website would suffice to increase their willingness to share personal data”.[459] Hierin schuilt wel een gevaar dat de betrokkene zijn persoonsgegevens verstrekt zonder de privacyverklaring te hebben gelezen. Tevens wijst onderzoek in de Verenigde Staten uit dat het lezen van een privacyverklaring maar één manier is om geïnformeerd te worden over de wijze waarop de verantwoordelijke de persoonsgegevens verwerkt. “Reading privacy notices is but one way consumers can learn about an organization’s information practices. Consumers may rely on alternative signals that provide assurances their information is safe such as privacy seal or the reputation or brand of the company”.[460]

5.3.2 De naamgeving, traceerbaarheid en de toegankelijkheid van de privacyverklaring

Voor de betrokkene moet het kenbaar zijn dat er een privacyverklaring op de website is geplaatst. Dit betekent dat de naamgeving van de (button van de) privacyverklaring eenduidig dient te zijn. In de praktijk worden door verantwoordelijken echter diverse benamingen voor de privacyverklaring gehanteerd. Papacharissi & Fernback concluderen dat de enkele vermelding van de term privacystatement de indruk wekt dat er garanties worden verstrekt ten aanzien van de bescherming van privacy, maar dat de inhoud veelal juist het oogmerk heeft om de belangen van de verantwoordelijke te beschermen. “Even though the etymology of the term *privacy statement* primes the user for a guarantee of

456 Vergelijk Jensen & Potts 2004, p. 471.
457 Dubbeld, p. 136.
458 Jensen & Potts 2004, p. 477.
459 Beldad, p. 155.
460 Milne & Culnan, p. 19.

privacy protection, the vocabulary of the statement itself frequently creates a legal safeguard for the company that seldom offers explicit reassurances of privacy protection".[461]
Het vereiste van traceerbaarheid veronderstelt dat de locatie van de privacyverklaring dusdanig is dat de betrokkene eenvoudig (de button van de) privacyverklaring kan waarnemen. "Unless policies are easily found and readily available to end users the quality of the policy doesn't matter".[462]
Met toegankelijkheid van de privacyverklaring wordt bedoeld dat de betrokkene op een eenvoudige en snelle wijze de beschikking over de privacyverklaring moet hebben. "In order to access and evaluate a site's privacy policy, the user must access at least two pages on the site: the home page and the page containing the privacy policy".[463] Het begrip toegankelijkheid houdt tevens in dat de betrokkene de privacyverklaring later alsnog (wederom) kan inzien. Dit betekent dat de privacyverklaring te allen tijde beschikbaar moet zijn op de website, maar ook dat de betrokkene de privacyverklaring moet kunnen opslaan.[464]

5.3.3 De vorm van de privacyverklaring

In paragraaf 2.3.3 kwam aan de orde dat de Groep Gegevensbescherming Artikel 29 adviseert om ten aanzien van de vorm van de privacyverklaring gebruik te maken van een gelaagde structuur. De informatie dient in maximaal drie trappen aan de betrokkene te worden verstrekt, aldus de Groep. Voorts bleek dat The Center for Information Policy Leadership het toepassen van gelaagde privacyverklaringen onderschrijft. Tevens is in die paragraaf gewezen op het gebruik van gelaagde privacyverklaringen door overheidsinstellingen binnen het Verenigd Koninkrijk en Australië.
McDonald et al. hebben onderzoek verricht naar het effect van gelaagde privacyverklaringen en komen onder meer tot de conclusie dat gelaagde privacyverklaringen leiden tot lagere accuratesse scores. Voorts concluderen ze dat het gebruik van deze gelaagde vorm ten koste gaat van transparantie. "As compared to natural language, we found that layered policies led to lower accuracy scores for topics not in the short layer"[465], "Both layered and Privacy Finder formats did improve times to answer, but not by much, and at the expense of accuracy for layered policies"[466] en "Results from the layered format suggest participants did not continue to the full policy when the information they sought was not available on the short notice. Unless it is possible to identify all of the topics users care about and summarize

461 Papacharissi & Fernback, p. 278.
462 Jensen & Potts 2004, p. 473.
463 Jensen & Potts 2004, p. 477.
464 Vergelijk in dezen de regelgeving met betrekking tot elektronische algemene voorwaarden, in het bijzonder artikel 6: 234 lid 1 sub c BW. Zie in dit kader Kamerstukken II 2001/02, 28 197, nr. 3, p. 59. Zie ook Maritius, p. 398.
465 McDonald et al., hoofdstuk 4.
466 McDonald et al., hoofdstuk 6.

to one page, the layered notice effectively hides information and reduces transparency".[467] McDonald adviseert ten aanzien van gelaagde privacyverklaringen: "We would neither suggest companies remove those formats from use nor would we suggest an aggressive push to adopt them".[468]

5.3.4 De inhoud, leesbaarheid en begrijpelijkheid van de privacyverklaring

In het kader van transparantie lijkt standaardisatie van de inhoud van privacyverklaringen (met andere woorden welke informatie wordt verstrekt aan de betrokkenen) ook een relevante factor te kunnen zijn. In het empirisch onderzoek is een diversiteit aan onderwerpen die in privacyverklaringen worden geadresseerd waargenomen. Er is in het voorgaande reeds enkele malen gerefereerd aan tabel 2.5 waarin de elementen zijn benoemd die volgens de Groep Gegevensbescherming Artikel 29 minimaal in een privacyverklaring moeten worden opgenomen. De vraag is echter of dit ook de onderwerpen zijn waar de betrokkene kennis van wil nemen. Onderzoek onder consumenten wijst immers uit dat privacyverklaringen niet die informatie verstrekken die zij graag zouden willen ontvangen.[469] De voornaamste reden voor de betrokkene om een privacyverklaring te lezen, lijkt – zo wijst onderzoek uit - te zijn gelegen in de wens te weten op welke wijze zijn persoonsgegevens worden gebruikt en beschermd. "The majority of those who participated in the study agreed that the need to know how their data would be used and protected is a primary motivation for reading an online privacy statement".[470] De drijfveer voor het lezen van een privacyverklaring is bezorgdheid over de wijze waarop persoonsgegevens worden verwerkt.[471] "Consumers are becoming increasingly concerned about how this information is being used, and frustrated over their lack of control. In attempt to reassure them, most large organisations now post online privacy policies spelling out what kinds of data they collect, what they do with it and how they protect it. The problem is that their efforts to be upfront about how they handle customer data can have the opposite effect. Customers are often bamboozled by long, complex notices packed with legal jargon and technical terms".[472]

De realiteit is echter dat privacyverklaringen veelal niet door betrokkenen worden gelezen. "The findings indicate that while respondents were generally aware of privacy policy statements, most do not take the time to read them".[473] "Desgevraagd antwoordden de

---

467 McDonald et al., hoofdstuk 6.

468 McDonald, p. 46.

469 Earp et al., p. 233. In het kader van het EU researchproject ENDORSE onderzoekt Van der Hof van welke informatie de betrokkene wil kennisnemen in een privacyverklaring. Prof. mr. S. van der Hof is werkzaam aan de afdeling eLaw@Leiden van de Universiteit Leiden.

470 Beldad, p. 154.

471 Vergelijk Milne & Culnan, p. 24.

472 Pedersen, p. 31.

473 Meinert et al., p. 135.

meeste deelnemers dat ze (bijna) nooit privacyverklaringen lezen (n=15)".[474] Dit beeld komt ook naar voren in onderzoek onder consumenten binnen de Europese Unie. "As a general rule, one third of EU consumers did not read any of the privacy notices on the websites they visited in the last 12 months, while another 15% said that they did this 'rarely'". Fewer than 3 in 10 EU consumers said that they 'often' or 'sometimes' read the privacy notices on websites".[475]

De redenen waarom betrokkenen de privacyverklaring niet lezen zijn divers. "Some shoppers do not want to sacrifice convenience to read a lengthy document, which often is filled with legal jargon. Some perceive that privacy disclosures, as a routine practice, are more or less the same. Still others believe that, by posting a privacy statement, organizations seek to escape liability or limit responsibility"[476] Een andere reden voor het niet lezen van privacyverklaringen heeft te maken met de factor tijd en de daarmee gerelateerde kosten. "Privacy policies should help reduce information asymmetries because companies share information with their customers. However, researchers also note that if the cost for reading privacy policies is too high, people are unlikely to read policies".[477] "One in five EU consumers who have not read privacy notices (33% of consumers – and 41% of those who did not indicate *not using the internet* – claimed not to have done so) invoked a lack of time as the main reason for not doing so, and for another 6% the main reason was that they thought the notices would have been too long".[478] Ook de reputatie of uitstraling van een bedrijf of website kan een reden zijn waarom een privacyverklaring niet wordt gelezen. In een onderzoek van TNO/IViR valt hierover te lezen: "In de discussie geven veel van de deelnemers die (bijna) nooit privacy policies lezen aan dat ze afgaan op de reputatie van een bedrijf, of een bedrijf betrouwbaar overkomt op basis van eigen ervaringen of die van bekenden, het uiterlijk van de website en de afkomst van de website".[479] "A further 7% declared that they trusted the provider and so did not need to read the privacy notices. Finally, 6% stated that they thought they were protected anyway by consumer laws. It should also be noted that half of those who did not read privacy notices invoked other

474 TNO/IViR, p. 54.

475 Flash Eurobarometer, p. 36.

476 Pan & Zinkhan, p. 337. Vergelijk Vu, Garcia, Nelson et al., p. 801. "Several users indicated indicated that they do not read the privacy policies because they either (a) trust well-known companies, (b) find the policies to be too long and confusing, or (c) do not care about who gets access to their information because it is not something they could control anyway"; Evenzo Jensen & Potts 2003, p. 6. "…the top two reasons given for not reviewing them are that they are too time-consuming and too hard to read."

477 McDonald & Cranor, p. 5 e.v. Zij komen voorts tot conclusie dat in de Verenigde Staten de kosten voor het lezen van privacyverklaringen kunnen worden begroot op $781 billion dollar per jaar, zie p. 2.

478 Flash Eurobarometer, p. 40.

479 TNO/IViR, p. 54. Het onderzoek is uitgevoerd door focusgroepen met een representatieve groep van 26 eindgebruikers in een testlab bij TNO te Delft (p. 48).

reasons than those provided in the pre-defined list of answers (such as 'no interest', 'do not care', 'did not provide any personal information' and 'was not prompted')".[480]

Redenerend vanuit het belang van transparantie over de gegevensverwerking is het belangrijk dat de betrokkene de privacyverklaring ook daadwerkelijk leest. Evenzo is het belangrijk dat de inhoud van de privacyverklaring leesbaar is.[481] "Making policies readable is of crucial importance, because difficult language, long and confusing policies all serve to trick and confuse the user"[482], en "It will therefore be continually important to ensure that policies are clear and readable".[483] Sommige verantwoordelijken maken gebruik van technieken om de leesbaarheid van de privacyverklaring te verbeteren. "The majority of companies do appear to use some other strategies to assist readability, such as numbered or bulleted lists, numerous headings to guide readers, conversational tone using 'we' and 'you', and hyperlinks of topics to allow effective use of 'white space' on the screen".[484]

Naast leesbaarheid, dient de privacyverklaring begrijpelijk te zijn. "For a Web site's privacy policy to be of value to users, the host organization must ensure that the information desired by the users is provided in a form that they will be able to comprehend easily".[485] Onderzoek onder EU-consumenten toont aan dat de begrijpelijkheid van privacyverklaringen voor verbetering vatbaar is. "Only 7% of those who read privacy notices found them 'very clear', while the largest proportion (45%) found them 'quite clear'". For about one third of those who read privacy notices in the last year, the content was judged 'quite unclear', with 11% of them finding it 'very unclear'".[486]
De inhoud van de privacyverklaring zal moeilijk te begrijpen zijn indien er gebruik wordt gemaakt van gecompliceerde zinnen en te veel moeilijke en ongebruikelijke woorden. "Patients will have a hard time understanding the notices because the writing styles use too many words per sentence, too many complicated sentences and too many complicated and uncommon words".[487] De betrokkene zal de inhoud van de privacyverklaring minder snel

480 Flash Eurobarometer, p. 40.

481 In deze paragraaf wordt een onderscheid gemaakt tussen leesbaarheid en begrijpelijkheid. Met leesbaarheid wordt bedoeld dat er geen moeilijke en lange zinnen worden gebruikt, en sprake is van een goede tekstuele structuur. Indien de inhoud van de privacyverklaring leesbaar is, wil dit niet zeggen dat deze als zodanig begrijpelijk is. De 'onwetende' betrokkene zal immers niet begrijpen wat wordt bedoeld met bijvoorbeeld 'Wbp, Cbp, meldplicht, cookies en inzage- en correctierecht'.

482 Jensen & Potts 2003, p. 5.

483 Jensen & Potts 2003, p. 8.

484 Kleen & Heinrichs, p. 352.

485 Vu, Chambers, Garcia et al., p. 811.

486 Flash Eurobarometer, p. 37.

487 Hochhauser, p. 1. Hochhauser onderzocht meer dan 30 privacyverklaringen die onder meer door zorgverzekeraars worden gebruikt op grond van de Privacy Rule. Deze Privacy Rule is uitgevaardigd door de U.S. Department of Health and Human Services ter implementatie van de vereisten zoals vastgelegd in de Health Insurance Portability and Accountability Act (HIPAA) of 1996.

lezen indien hij vermoedt of merkt dat de inhoud moeilijk te begrijpen is. “If the notice is not perceived as comprehensible, then it will be less likely to be read”.[488] De begrijpelijkheid van een privacyverklaring zal in het geding komen indien de privacyverklaring alleen wordt gebruikt om te voldoen aan de wettelijke verplichtingen. “First, like product labels and warnings, online privacy may be used for compliances purposes. As a result, organizations write privacy notices to be exhaustive and not necessarily to be accessible to consumers and informative”.[489] De begrijpelijkheid van een privacyverklaring is mede afhankelijk van de wijze waarop de inhoud van de privacyverklaring wordt weergeven. “The fact that comprehension scores were still low when participants were able to search for the information in the policy suggests that important information in privacy policies is not stated in a way that can be easily understood by users”.[490] De inhoud van een privacyverklaring dient derhalve specifiek te worden weergegeven. “The study results are indicative of the need to not simply state how personally identifiable and non identifiable information will be used but to do so with specificity and clarity”.[491] Daarbij blijkt dat betrokkenen zich met name richten op de eerste zinnen van de privacyverklaring en op de eerste woorden van elke paragraaf uit de privacyverklaring. “The aggregate gaze data showed that, when reading privacy policies, participants paid particular attention to the first few sentences in the policy, the first few words of each paragraph in the policy and information in bold or underlined”.[492] Vail et al. benadrukken dat er een verschil is tussen de perceptie (User Perception) van de betrokkene ten aanzien van de inhoud van de privacyverklaring en de begrijpelijkheid (User Comprehension) van de privacyverklaring. In hun onderzoek concluderen zij dat perceptie en begrijpelijkheid niet samenvallen en daarmee niet altijd wat betreft de beoordeling dezelfde kwalificatie opleveren. Vail et al. vinden dit verontrustend daar de betrokkene klaarblijkelijk geneigd is om een bedrijf te vertrouwen terwijl de privacyverklaring van het bedrijf gebreken vertoont wat betreft leesbaarheid.[493]

Een relevante factor bij transparantie lijkt verder de specifieke doelgroep van de website. “Generally, men were more likely than women to read privacy notices on websites”.[494] Jeugdigen begrijpen of interpreteren de inhoud van een privacyverklaring mogelijk anders dan volwassenen. Dit is waarschijnlijk de reden waarom de Europese Commissie stelt dat de inhoud van het privacybeleid, en daarmee de inhoud van de privacyverklaring, qua bewoording dient te zijn afgestemt op de relevante doelgroep.[495]

---

488 Milne & Culnan, p. 24.
489 Milne & Culnan, p. 24.
490 Vu, Chambers, Garcia et al., p. 811.
491 Papacharissi & Fernback, p. 278.
492 Vu, Chambers, Garcia et al., p. 806.
493 Vail et al., p. 451.
494 Flash Eurobarometer, p. 36.
495 COM (2012) 11 final.

> Article 11 Transparent information and communication
> 2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.

Bovendien blijkt dat privacyverklaringen meer door ouderen dan door jongeren worden gelezen. “Older respondents are more likely to read online privacy statements compared to younger respondents”.[496] Tevens wijst onderzoek uit dat er een negatieve relatie bestaat tussen de opleiding van de respondenten enerzijds en hun intentie om online privacyverklaringen te lezen anderzijds: “...respondents with lower levels of education are more likely to read online privacy statements than those with higher levels of education…”.[497] Echter, onderzoek onder EU-consumenten wijst uit dat jongeren vaker privacyverklaringen lezen in vergelijking met andere sociaal-demografische groepen. “Equally, Young consumers, those who are self employed or employees, and those who have stayed longer in full time education (or are still studying) tended to read these privacy notices more often than other sociodemographic groups”.[498]

Transparantie ten aanzien van de privacyverklaring betekent tevens dat de betrokkene kennis kan nemen van eventuele latere aanpassingen in de inhoud van een privacyverklaring. Veelal wordt een privacyverklaring afgesloten met de mededeling dat “het aanbeveling verdient om de privacyverklaring geregeld te raadplegen, zodat u van wijzigingen op de hoogte bent”.[499] Het is niet onwaarschijnlijk dat de betrokkene in de praktijk dit ‘regelmatig raadplegen’ nalaat. Anderzijds zijn er situaties bekend waarbij de verantwoordelijke op een actieve wijze de betrokkene informeert. Een illustratie van een situatie waarin de verantwoordelijke op enig moment de wijze van verwerken aanpaste zonder de betrokkenen hierover te informeren, betreft de sociale netwerksite Facebook. In december 2009 gaf Facebook de betrokkene de mogelijkheid om nauwkeuriger te kunnen bepalen wie welke gegevens op zijn profiel mocht bekijken. Ook kon de betrokkene standaardinstellingen makkelijker aanpassen. In werkelijkheid werden de instellingen automatisch omgezet waardoor profielinformatie, foto’s en vriendenlijsten standaard zichtbaar werden, en liet Facebook het na om de betrokkene hierover te informeren.[500] Voor het bevorderen van transparantie lijkt het in ieder geval gewenst dat er meer eenduidigheid

---

496 Beldad, p. 156.

497 Beldad, p. 156. Milne & Culnan komen tot eenzelfde conclusie, Milne & Culnan, p. 21.

498 Flash Eurobarometer, p. 36.

499 Of woorden van gelijke strekking. Zie bijvoorbeeld www.abnamro.nl, www.centraalbeheer.nl, www.vliegtickets.nl, www.vliegwinkel.nl en www.babysbest.nl.

500 De Groep Gegevensbescherming Artikel 29 heeft Facebook laten weten dat het fundamenteel gewijzigd hebben van de standaard instellingen onacceptabel is. Groep Gegevensbescherming Artikel 29, Persbericht, 12 mei 2010, Brussel.

bestaat in de wijze waarop de betrokkene wordt geïnformeerd in geval van een latere wijziging van de inhoud van de privacyverklaring.[501]

Niet zelden komt het voor dat informatie aangaande de verwerking van persoonsgegevens op een website 'her en der' verspreid is. Zo kan het voorkomen dat zowel een privacyverklaring op de website is geplaatst, als elektronische algemene voorwaarden waarin bepalingen met betrekking tot de verwerking van persoonsgegevens zijn opgenomen. Daarbij is het niet ondenkbaar dat in dat geval de bepalingen uit de privacyverklaring enerzijds en de algemene voorwaarden anderzijds met elkaar conflicteren of 'dubbelop' zijn.[502] Vanuit het oogpunt van transparantie is een dergelijke situatie niet wenselijk.

Tenslotte laat onderzoek zien dat transparantie valt te bevorderen door consumenten en andere betrokkenen voor te lichten over de wijze waarop zij privacyverklaringen moeten begrijpen. "Consumer education enhances transparency by helping individuals better understand privacy notices, when choice may be an option, and when access may be available to them".[503]

5.4 Initiatieven ter bevordering van de transparantie van privacyverklaringen

In de vorige paragraaf is diverse malen verwezen naar empirisch onderzoek dat in de Verenigde Staten is uitgevoerd naar het gebruik van privacyverklaringen. Als we verschillende onderzoeken die gedurende een periode van 7 jaar zijn uitgevoerd in tijd ordenen, zijn daarin op hoofdlijnen de volgende conclusies te lezen.

[2003] Privacyverklaringen worden verkeerd begrepen. "We found that despite their strong concerns about online privacy, most adults who use the internet at home misunderstand the purpose of a privacy policy".[504]
[2003] Het gebruik van privacyverklaringen is een ineffectieve manier om online privacy te beschermen. "The practice of privacy policies as it stands today is an ineffective way to protect users privacy online. Most users rarely consult privacy policies, and when they do they often find them unintelligible".[505]

---

501 De verantwoordelijke zou bijvoorbeeld de betrokkene per e-mail kunnen informeren dat de inhoud van de privacyverklaring is gewijzigd.
502 Zie bijvoorbeeld de privacyverklaring en de disclaimer van Prolife.nl.
503 The Center for Information Policy Leadership 2011, p. 8.
504 Turow, p. 33.
505 Jensen & Potts 2003, p. 8.

[2003] Het gebruik van een privacyverklaring heeft eerder een negatief dan een positief effect. “As the practice stands today, having a privacy policy linked to a site, or displaying a privacy seal, may have more of a negative than a positive effect on users. The simple fact that a site has a policy or a seal does not mean they protect users privacy more than a site without, though users may make that assumption”.[506]

[2004] Privacyverklaringen worden nagenoeg niet gelezen. “From a small survey done in university setting we found from log file analysis that for a standalone website requiring registration, virtually no-one read the policy”.[507]

[2004] Vanwege de vorm, plaatsing en juridische status biedt de privacyverklaring geen ondersteuning aan de betrokkene indien hij privacygerelateerde beslissingen moet nemen. “The form, location and legal context of policies make them essentially unusable as decision-making aids for a user concerned about privacy”.[508]

[2004] De huidige privacyverklaringen zullen flink op de schop moeten. “The results of our study also indicate that current privacy notices need to undergo a major reform”.[509]

[2005] Een privacyverklaring is geen adequaat instrument om het niveau van feitelijke privacybescherming te kunnen bepalen. “Therefore, the privacy statement becomes an inadequate measure of privacy protection, designed to sustain an illusion of concern over information collected”.[510]

[2007] Het begrip onder betrokkenen van de inhoud van privacyverklaringen was tamelijk laag. “Participants’ comprehension of information contained within privacy policies was found to be quite low”.[511]

[2008] De huidige privacyverklaringen zijn niet toereikend om het beleid van de organisatie helder te maken. “The results presented in this paper illustrate that current privacy policy representations are not sufficient for conveying an organization’s privacy practices”.[512]

[2008] De wijze waarop privacyverklaringen worden geïmplementeerd op de websites van organisaties laat te wensen over. “From a usability perspective, there is considerable room for improvement in the design of organizations’ Web sites with respect to the amount and types of person information solicited and the implementation of privacy policies”.[513]

[2009] De huidige privacyverklaringen falen in hun doelstelling. “In short, today’s online privacy policies are failing…”.[514].

---

506 Jensen & Potts 2003, p. 8.
507 Jensen & Potts 2004, p. 477.
508 Jensen & Potts 2004, p. 477.
509 Milne & Culnan, p. 25.
510 Papacharissi & Fernback, p. 278 e.v.
511 Vu, Chambers, Garcia et al., p. 802.
512 Vail et al., p. 452.
513 Proctor et al., p. 1.
514 Kelly et al. 2009, p. 1.

[2010] Privacyverklaringen zijn veelal onduidelijk, ontberen uniformiteit en zijn te lang. "…,privacy notices are often opaque, lack uniformity, and are too long and difficult to navigate".[515]
[2010] Het transparantieniveau van de huidige privacyverklaringen is laag. "… the level of effective transparency and awareness of current privacy practices is low". "The shortcomings of many privacy policies are widely recognized: they can be dense, lengthy, written in legalese and overwhelming to the few consumers who actually venture to read them".[516]

Al met al laten voorgaande conclusies niets aan duidelijkheid te wensen over: de door mij hiervoor geïdentificeerde aspecten om te komen tot transparante privacyverklaringen worden niet of nauwelijks in de Verenigde Staten toegepast en leveren wat betreft privacybescherming in den brede niet het gewenste resultaat op. Het gebrek aan transparantie heeft in de Verenigde Staten geleid tot de hypothese dat de gewenste mate daarvan mogelijk kan worden gerealiseerd door het ontwikkelen van gestandaardiseerde privacyverklaringen. Aldus zijn diverse initiatieven gelanceerd om te komen tot gestandaardiseerde privacyverklaringen.

In de Verenigde Staten hebben financiële instituties op grond van de Gramm-Leach-Bliley Act de plicht om privacyverklaringen te verstrekken aan hun klanten.[517] Aanhakend bij deze verplichting is Kleimann een project gestart om een (papieren) gestandaardiseerde privacyverklaring te ontwikkelen.[518] Het project had tot doel te analyseren waarom consumenten de gehanteerde privacyverklaringen niet lezen of (lijken te) begrijpen. Bovendien had Kleimann als ambitie aan de hand van zijn onderzoeksresultaten een privacyverklaring te ontwikkelen die wel door consumenten zou worden begrepen. "The project objective was to explore the reasons why consumers don't read and understand privacy notices and to use this research to develop paper-based, alternative privacy notices - or components of notices - that consumers can understand and use". Levy & Hastak hebben vervolgonderzoek gedaan naar de mate waarop consumenten gestandaardiseerde privacyverklaringen begrijpen en daarin, naast andere gestandaardiseerde privacyverklaring modellen, het KCG model van Kleimann betrokken. De resultaten tonen aan dat "the KCG Table notice shows a performance superiority for harder tasks that require complex comprehension, such as giving logically sufficient reasons for choice (Judgment Quality), or deciding how much information sharing is being done once opt-outs are exercised (AfterOptOut)".[519] Hiernaast laat hun onderzoek ook zien dat het KCG model in vergelijking

515 Federal Trade Commission, p. 70.
516 Department of Commerce, p. 31.
517 U.S. Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA).
518 Kleimann 2006, p. ii.
519 Levy & Hastak, p. 1.

met een korte privacyverklaring minder scoort indien er sprake is van een eenvoudiger situatie.[520] Het KCG model lijkt in ieder geval de leesbaarheid ten goede te komen. “The 2006 Kleimann report on GLB financial privacy notices found that subheadings and standard formats dramatically improved readability”.[521] Vervolgens heeft Kleimann een web-based gestandaardiseerde privacyverklaring ontwikkeld. Het model hiervoor, zoals opgenomen in Bijlage G, werd in 2009 gepresenteerd aan de Federal Trade Commission. De resultaten van onderzoek naar dit model lijken bemoedigend: “The migration of the paper financial privacy notice prototype to a web-based version successfully retained high performance in comprehension, design integrity, navigation, and task completion. At the same time, the online medium facilitated an updated design that optimized the dynamic and functional possibilities of the web. Collapsing, combining, re-ordering, and enhancing the visual nature of content and the key elements allowed the notice to meet participants’ needs when interacting with the information online”.[522]

Ook Vail et al. deden onderzoek naar het effect van gestandaardiseerde privacyverklaringen. Zij onderscheidden ‘typical online privacy policies’ (TOPPs) en ‘alternative privacy policies’ (APPs).[523] De navolgende varianten van online privacy policies op websites zijn door Vail et al. aan respondenten gepresenteerd:[524]

1. *Policy:* Deze variant betreft de oorspronkelijke privacy policy die is verkregen van de website, en betreft een TOPP.
2. *Goal/vulnerability statements*: In deze APP-variant wordt het te voeren privacybeleid uitgedrukt in een lijst met privacydoelstellingen (*privacy goals*) en -kwetsbaarheden (*vulnerability statements*).
3. *Categorical*: In deze weergave zijn de privacydoelstellingen en -kwetsbaarheden gecategoriseerd. De respondent kan op een categorie klikken, waarna in ‘bulletvorm’ een lijst van doelstellingen/kwetsbaarheden verschijnt die relevant zijn voor de betreffende categorie. Het betreft hier een APP-variant.
4. *Goals/vulnerabilities in policy*: In deze APP-variant wordt de originele privacy policy (*Policy*) getoond, waarbij de privacy doelstellingen en kwetsbaarheden zijn vet gedrukt en ‘gehighlight’. Er verschijnt een pop-up scherm indien de respondent zijn muis beweegt over de vetgedrukte en ‘gehighlighte’ doelstellingen en kwetsbaarheden. In het pop-up scherm worden andermaal de doelstellingen en kwetsbaarheden getoond.

---

520 Levy & Hastak, p. 16. “On the other hand, the shorter Sample Clause Notice performs better on simpler tasks and actually performs better than the KCG Table Notice on the one task based on skimming the notice for the right answer (Contact Mode)”.

521 McDonald et al., p. 2.

522 Kleimann 2009, p. 16.

523 Vail et al., p. 445. In het onderzoek zijn 3 websites van organisaties die zich bevinden binnen het domein van de gezondheidszorg als onderzoeksobject genomen.

524 Vail et al., p. 445 e.v.

Uit het onderzoek volgt onder meer dat de respondenten zich daar waar het de bescherming van persoonsgegevens betreft zekerder voelen (*User Perception*) wanneer de variant Policy wordt gebruikt, gevolgd door de variant *Goals/vulnerabilities in policy.*[525] Daarentegen laat het onderzoek ook zien dat de privacy notice beter wordt begrepen (*User Comprehension*) indien gebruik wordt gemaakt van een gestandaardiseerd model, te weten de variant *Categorical*, gevolgd door de variant *Goal/vulnerability statements*.[526]

Kelly et al. hebben zich in hun onderzoek, dat ziet op het ontwikkelen van een gestandaardiseerde privacyverklaring, laten inspireren door studies die zijn uitgevoerd in het kader van etikettering van producten die voedingswaarden bevatten. In het bijzonder hebben zij gekeken naar het ontwerp van het etiket en de acceptatiegraad daarvan door de consument.[527] Relevant om hierbij te vermelden is dat in de Verenigde Staten de Nutrition Labeling and Education Act van kracht is.[528] Uitgaande van deze wet, stellen Kelly et al.: "We believe that we should focus on providing a technology that is similar in ways to nutritional labels that are on food products. Consumers are very aware that when selecting an item at the grocery store there are a number of choices and their nutritional values differ. Because there is a legislated standard label consumers are able to easily compare different products and make an informed decision on what will stock their pantries".[529] Ciocchetti stelt in dezen: "Labels will also standardize the look and feel of privacy policies and be located on a company's homepage", en "The goal of a Label regime is for visitors to open a specific Web page, encounter the Label, read and understand its meaning and, hopefully, find guidance on whether to submit personally identifying information".[530] Het voorstel om gestandaardiseerde privacyverklaringen te ontwikkelen naar voorbeeld van een nutritional label vindt steun bij FTC Commissioner Anthony. "The NLEA food labels and the Energy Guides provide excellent examples of standardized formats that convey complex but important information for consumers. A number of benefits that would flow from standardizing the formats including creating a level playing field for industry and providing consumers with easy to understand information about the information sharing practices of the companies with which they do business. A standardized privacy format could provide consumers more confidence in the online marketplace that will only be good for business in the long run".[531] Milne & Culnan merken over de aanpak overeenkomstig voedseletikettering op: "If privacy notices are to take on the importance and usefulness of nutritional label, a simplified, unified format that presents information in a condensed and accessible format is

525 Vail et al., p. 448.
526 Vail et al., p. 449.
527 Kelly et al. 2009, p. 1.
528 Nutrition Labeling and Education Act of 1990 (NLEA).
529 Kelly et al. 2008, p. 1.
530 Ciocchetti, p. 25.
531 Anthony.

needed".[532] Ciocchetti benadrukt dat "NELA labels have successfully raised consumer awareness regarding the nutritional value of different foods. The privacy nutrition label would be a direct descendant of these NELA labels and would target consumer awareness of privacy practices. It is helpful to consider Labels as a type of stoplight for Web surfers. Each Label will indicate, in a standardized manner, whether a company's privacy practices are privacy-protective (indicating it is safe to go forward) or privacy-invasive (stop!)".[533]
De door Kelly et al. vervaardigde gestandaardiseerde privacyverklaring wordt in tabel- en blokvorm gepresenteerd, daarbij gebruikmakende van kleurstellingen. Per rij wordt gepreciseerd welke informatie wordt verzameld (bijvoorbeeld financiële of demografische informatie), en per kolom wordt benoemd waarvoor de verzamelde informatie wordt gebruikt (bijvoorbeeld voor het uitvoeren van diensten of marketingactiviteiten). Het model is opgenomen in Bijlage H. Uit het onderzoek van Kelly et al. volgt dat de gestandaardiseerde privacyverklaring 'over all' beter scoort dan de full text of gelaagde privacyverklaringen.[534] Tevens zijn de eerste onderzoeksresultaten met betrekking tot het gebruik van privacyverklaringen die gebaseerd zijn op het 'nutrition label concept' bemoedigend. "Early results testing a new format for privacy policies based around a nutrition label concept are encouraging".[535] In Europa heeft de Groep Gegevensbescherming Artikel 29 nog geen standpunt ingenomen ten aanzien van dit model. Naar het lijkt voldoet het wel aan de visie van de Groep dat informatie met betrekking tot de verwerking van persoonsgegevens rechtstreeks op het scherm dient te worden verstrekt, zonder dat de betrokkene zelf actie moet ondernemen om toegang te krijgen tot de informatie.[536]

Een ander initiatief dat tracht om transparantie te bevorderen in relatie tot privacyverklaringen betreft het PRIME Project uitgevoerd binnen de kaderprogramma's van de Europese Commissie.[537] Dit project richt zich onder meer op het ontwikkelen van 'human computer interfaces'. "Door middel van zeer eenvoudige en snel herkenbare visuele pictogrammen kan voorkomen worden dat gebruikers (als ze dat al zouden doen) lange teksten in juridisch jargon moeten lezen alvorens de beslissing te nemen naar de gewenste website door te klikken".[538] Min of meer soortgelijk is het initiatief Privacy Finder.[539] De Privacy Finder is een privacy-enhanced zoekmachine. De zoekresultaten worden gebaseerd

532 Milne & Culnan, p. 25.
533 Ciocchetti, p. 25.
534 Kelly et al. 2010, p. 9.
535 McDonald et al., hoofdstuk 6. Zie ook Kelly et al. 2009, p.9 e.v.
536 Groep Gegevensbescherming Artikel 29-2000, p. 52.
537 Privacy and Identity Management for Europe, EU research project.
538 Borking, p. 214.
539 De Privacy Finder is ontwikkeld door het bedrijf AT&T en doorontwikkeld door het CMU Usable Privacy and Security laboratory (Carnegie Mellon University). McDonald, p. 31.

op 'computer readable' privacyverklaringen.[540] De score van de privacyverklaring wordt weergegeven met behulp van groene vakjes. Hoe meer groene vakjes (maximaal 4), des te optimaler is de overeenstemming tussen het door de betrokkene gewenste privacyniveau en het privacybeleid van de website.[541] Ook Antón et al. werken aan een methodiek om privacyverklaringen te kunnen classificeren, en aan de hand daarvan privacyverklaringen te kunnen analyseren en vergelijken.[542]

Ter bevordering van transparantie is er verder ook software ontwikkeld waarmee privacyverklaringen kunnen worden gegenereerd.[543] Hiernaast bestaan er 'guidelines' die ondersteuning bieden bij het ontwikkelen van privacyverklaringen.[544] Tot slot wordt gewezen op de zogeheten privacy seals. Door een, veelal onafhankelijke, organisatie wordt in dat geval een aantal voorwaarden gesteld met betrekking tot de verwerking van persoonsgegevens.[545] Een verantwoordelijke die voldoet aan deze voorwaarden mag vervolgens een privacy seal op zijn website plaatsen, daarmee kenbaar makend dat hij voldoet aan de privacystandaarden van die onafhankelijke organisatie. Het gebruik van privacy seals kent, aldus deskundigen, echter een aantal beperkingen:

- "The most serious obstacle to web seal success is that few companies value seals enough to voluntarily adopt them";[546]
- "Another problem with privacy seals is that they limit privacy choices to a take-it-or-leave-it proposition. Consumers who prefer a higher privacy standard than the one propagated by the seal organization must revert to interpreting privacy policies";[547]
- "These seals often do not address the content of the policy, but rather the fact that the company has a policy, that this policy addresses a minimum set of issues, and that the company adheres to the stated policy. Users often mistake these seals to mean something about the level of privacy protection offered, which is not the case";[548]

---

540 De zogeheten P3P privacyverklaringen. "De P3P-standaard is ontworpen door het World Wide Web Consortium (W3C) en maakt het mogelijk dat op een website de bezoeker duidelijk wordt gemaakt welke persoonsgegevens worden verzameld en op welke wijze die gegevens zullen worden gebruikt". Borking, p. 221. Zie ook Jensen & Potts 2003, p. 7; .www.w3.org/P3P; zie tevens Kelly et al. 2008.

541 Zie voor meer informatie www.privacyfinder.org.

542 Antón et al.

543 Zie bijvoorbeeld de privacygenerator van de OESO en van Thuiswinkel.org.

544 Zie bijvoorbeeld "Guidelines for Online Privacy Policies" van de Online Privacy Alliance; Cbp Richtsnoeren Persoonsgegevens op internet; The Center for Information Policy Leadership 2007.

545 In de Verenigde Staten zijn TRUSTe (www.truste.com) en BBBOnLine (www.bbb.org/online/) de meest gebruikte privacy seals. In Nederland is een soortgelijk initiatief gestart door het NIVRA is samenwerking met NOREA. Zie de website www.privacy-audit-proof.nl.

546 Oussayef, p. 128.

547 Oussayef, p. 128.

548 Jensen & Potts 2003, p. 4.

- “Though seals may encourage more complete policies, they do not necessarily mean better protection for the user”.[549]

Een beperking van privacyverklaringen en de voornoemde initiatieven is dat de betrokkene niet of nauwelijks kan controleren of de verantwoordelijke ook daadwerkelijk nakomt wat hij in de privacyverklaring heeft toegezegd. “Users of a website are given a policy to read, in essence a list of promises and disclosures about how their information will be used and treated. What takes place behind the scenes is hidden from the user, and so it is a daunting task to determine whether a site abides by its own policy”.[550] De verantwoordelijke zou zich dan ook moeten verantwoorden over de wijze waarop hij persoonsgegevens (heeft) verwerkt. Dit uitgangspunt is onlosmakelijk verbonden met het beginsel van accountability waar de Europese Commissie een sterk voorstander van lijkt te zijn. Het accountability beginsel zal daarom in de volgende paragraaf nader worden besproken.

5.5 Accountability

Behalve aan het thema transparantie refereert de Europese Commissie in het debat over herziening van de Privacyrichtlijn aan het belang van accountabilty. De Commissie stelt in de eerder besproken mededeling uit 2010 dat moet worden nagegaan hoe het best kan worden verzekerd dat de verantwoordelijke *de facto* beleid voert en mechanismen instelt ter naleving van de regels inzake gegevensbescherming.[551] De Commissie overweegt derhalve de invoering van het accountability beginsel in de herziene Richtlijn. In het voorstel inzake herziening van de Privacyrichtlijn uit 2012 wordt dit concreet tot uitdrukking gebracht. “Article 22 takes account of the debate on a ‘principle of accountability’ and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance”.[552]

> Article 22 Responsibility of the controller
> 1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

Het voornemen van de Commissie om accountability te introduceren lijkt op brede steun te kunnen rekenen. Zo stelt de Groep Gegevensbescherming Artikel 29 dat door het

549 Jensen & Potts 2003, p. 5.
550 Jensen & Potts 2003, p. 6.
551 COM (2010) 609 definitief, p. 13.
552 COM (2012) 11 final, p. 10.

accountability beginsel een plaats te geven in de herziene Privacyrichtlijn, de verantwoordelijke ertoe wordt aangezet om maatregelen in te voeren die in de praktijk leiden tot een daadwerkelijke bescherming van de persoonsgegevens.[553] Cavoukian stelt in dit kader: "In today's world of ubiquitous data availability, trust is increasingly a function of how well organizations manage personal information in their care transparently and responsibly, and are able to demonstrate their diligence to customers, partners, shareholders, and regulators. Putting into place effective policies and mechanisms to ensure compliance with data protection laws is essential".[554] Het Nederlands Genootschap Functionarissen Gegevensbescherming merkt in een reactie over het voornemen van de Europese Commissie het volgende op: "The NGFG supports the accountability principle. Based on proven positive effect of the appointment of DPOs on data protection, the NGFG believes that this principle can lead to establishing safeguards and mechanisms which make data protection compliance more effective while reducing and simplifying certain administrative formalities, such as notifications".[555] Ook het kabinet onderschrijft het belang van het accountability beginsel. Het eerder aangekondigde voornemen om dit beginsel nader uit te willen werken in de Wbp heeft het kabinet echter op een lager plan gezet. "Het kabinet ziet in de mededeling van de Commissie overigens aanleiding om een aantal voornemens die zijn neergelegd in het meergenoemde kabinetsstandpunt naar aanleiding van de evaluatie van de Wbp en het rapport van de Adviescommissie veiligheid en de persoonlijke levenssfeer vooralsnog niet in de vorm van Nederlandse wetgeving ten uitvoer te leggen. Het betreft hier met name de uitwerking van het accountability beginsel in de Wbp (daaronder verstaat het kabinet het stimuleren van het opzetten of uitbreiden van een eigen intern privacybeleid door ondernemingen bij wijze van zelfregulering, in ruil voor het verlichten van administratieve lasten; het bedrijfsleven zou daarbij in de visie van het kabinet optimale keuzevrijheid moeten hebben met betrekking tot de wijze waarop dit beleid wordt ingericht; wellicht is dit ook voor de overheid denkbaar),…".[556] Ook breder – dat wil zeggen buiten de specifieke situatie van de bescherming van persoonsgegevens – wordt het belang van accountability in de huidige samenleving onderstreept. Zo stelt de WRR in het rapport *iOverheid* dat het belang van accountability in deze tijd moeilijk overschat kan worden. "Waar eenvoudige en eenduidige sturingsfilosofieën in de ogen van velen onvermijdelijk stuklopen op maatschappelijke complexiteit, biedt een procesbeginsel als accountability uitkomst. Het eist slechts een controlerelatie tussen een forum en een actor. Zo kunnen degenen wiens belangen in het forum behartigd worden, vat krijgen op het opereren van de actor in kwestie".[557]

---

553 Groep Gegevensbescherming Artikel 29-2010 (II), p. 6. Zie in dit kader ook het persbericht van het Cbp d.d. 19 juli 2010 "Vice-president Europese Commissie Reding bepleit versterking privacytoezichthouders".

554 Cavoukian 2011, p. 1.

555 NGFG, p. 3.

556 Kamerstukken II 2010-2011, 32761, nr. 1, p. 15.

557 WRR rapport *i*Overheid, p. 85.

Het accountability beginsel werd overigens al in 1980 door de OESO gedefinieerd als een van de acht principes in relatie tot de bescherming van privacy en individuele vrijheden: “A data controller should be accountable for complying with measures which give effect to the principles stated above”.[558] Bijna 30 jaar later, in 2009, werd het beginsel weer nieuw leven ingeblazen en wel in de Madrid Resolution.[559] Recentelijk heeft de Raad van Europa consultatieronden afgerond over een mogelijke herziening van de Conventie 108[560], hetgeen heeft geresulteerd in een voorstel om accountability mechanismen te introduceren in de Conventie 108.[561]

Als we kijken naar de definiërende elementen van accountability, dan lezen we dat de Canadese toezichthouder Cavoukian de navolgende opsomt:[562]

1. An organization’s commitment to accountability and adoption of internal policies consistent with external criteria;
2. Mechanisms to put privacy policies into effect, including tools, training, and education;
3. Systems for internal ongoing oversight and assurance reviews and external verification;
4. Transparency and mechanisms for individual participation;
5. The means for remediation and external enforcement.

Bij accountability ligt de nadruk op het inzichtelijk maken van de manier waarop verantwoordelijken invulling geven aan hun verantwoordelijkheden, alsmede het controleerbaar maken daarvan.[563] “Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions”.[564] “Accountability does not redefine privacy, nor does it replace existing law or regulation; accountable organisations must comply with existing applicable law. But

558 OECD, Principle 14.

559 Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, which was welcomed by the International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5 November 2009. Zie in dit kader ook Moerel, p. 384.

560 De Raad van Europa heeft het recht op gegevensbescherming uitgewerkt in Conventie 108 (naast de artikelen 8 en 10 EVRM en, door het EHRM, in de jurisprudentie ter zake) die in 1981 tot stand kwam. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108 – Automatic processing of Personal Data, 28.I.1981.

561 Raad van Europa, p. 11.

562 Cavoukian 2009, p. 5. Zie in dit kader ook The Center for Information Policy Leadership 2009, p. 11 e.v.

563 Groep Gegevensbescherming Artikel 29-2010 (II), p. 9.

564 Cavoukian 2009, p. 5. De door haar aangehaalde definitie is de werkdefinitie van accountability die werd gehanteerd door een groep van experts in het kader van het Galway Accountability Project.

accountability shifts the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified privacy objectives".[565]

Concreet wordt met accountability het effect beoogd, aldus de Groep Gegevensbescherming Artikel 29, dat er interne maatregelen en procedures ten uitvoer worden gelegd om gevolg te geven aan bestaande beginselen voor gegevensbescherming en de doeltreffendheid van die beginselen te waarborgen. Bovendien geldt de verplichting om de tenuitvoerlegging op verzoek van de gegevensbeschermingsautoriteiten aan te tonen.[566] Ook Bigo et al. zitten op deze lijn. "In broad terms, the principle of accountability places upon data controllers the burden of implementing within their organisation's specific measures to ensure that data protection requirements are met while executing their processing of personal data. Such measures could include anything from the introduction of a data protection officer to implementing Data-Protection Impact Assessments or employing privacy-by-design system architecture".[567]

The Center for Information Policy Leadership heeft 9 beginselen geïdentificeerd die de verantwoordelijke in het kader van accountability in zijn organisatie zou moeten implementeren. Een beginsel betreft het opstellen en implementeren van een privacy policy. "An organisation should develop, implement and communicate to individuals data privacy policies informed by appropriate external criteria found in law, regulation, or industry best practices, and designed to provide the individual with effective privacy protections".[568] Het Internet kan een duidelijke rol spelen bij het invulling geven aan accountability. Zo stelt de Groep Gegevensbescherming Artikel 29 dat een hoger verantwoordingsniveau wordt bereikt indien de verantwoordelijke zijn privacybeleid via het Internet kenbaar maakt.[569] Met andere woorden, een maatregel die de verantwoordelijke vanuit het accountability oogpunt kan nemen is het plaatsen van een privacyverklaring op zijn website. In dit kader is relevant de opmerkingen van Bennet. "Many current accountability mechanisms simply focus on the first, the stated privacy policies, and compare what is said on a website, or in a code of practice, to a stated norm. Claims of compliance are based on an analysis of words, rather than processes or practices".[570] Het in een privacyverklaring verklaren op welke wijze de verantwoordelijke voldoet aan de normen en verplichtingen uit de Wbp alleen is derhalve niet voldoende. Accountability houdt volgens Bennet tevens in dat wordt gecontroleerd of de verantwoordelijke ook daadwerkelijk hetgeen hij in de privacyverklaring heeft verklaard naleeft. "Few organizations, however, subject themselves to a verification of practices. Do

565 The Center for Information Policy Leadership 2009, p. 3.
566 Groep Gegevensbescherming Artikel 29-2010 (II), p. 6.
567 Bigo et al., p. 111.
568 The Center for Information Policy Leadership 2010, p. 6.
569 Groep Gegevensbescherming Artikel 29-2010 (II), p. 16.
570 Bennet 2010, p. 6.

the policies work?"[571] Dit betekent tevens dat de verantwoordelijke organisatorische en technische maatregelen in zijn organisatie moet implementeren die waarborgen dat conform de inhoud van de privacyverklaring wordt gehandeld. "The organisation must establish performance mechanisms to implement the stated privacy policies".[572] "The accountable organization deploys and monitors mechanisms and internal programs that ensure its privacy policies are carried out".[573] Illustratief is de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen, waarin is bepaald dat belang wordt gehecht aan een correcte naleving van de regels van de Wbp en de gedragscode. De financiële instellingen hebben daartoe een systeem van zelfevaluatie geïmplementeerd op basis waarvan risicoanalyses worden gemaakt. Tevens is een financiële instelling gehouden om interne instructies op te stellen en te implementeren waarin nader wordt aangegeven op welke wijze persoonsgegevens worden verwerkt.

> Artikel 10 Gedragscode Verwerking Persoonsgegevens Financiële Instellingen
> 10.1 Financiële instellingen hechten belang aan een correcte naleving van de regels van de WBP en Gedragscode. In dat kader hebben Financiële instellingen een stelsel van zelfevaluaties geïmplementeerd door middel waarvan periodiek risicoanalyses worden gemaakt met betrekking tot de naleving van de WBP en deze Gedragscode. Onderdeel hiervan is dat door een Financiële instelling wordt vastgesteld op welke wijze en hoe frequent de diverse onderdelen van de Financiële Instelling worden gecontroleerd op correcte naleving van de WBP en de Gedragscode, alsmede het opstellen van rapportages.
> 10.2 Ter bevordering van de naleving van de regels van de WBP en Gedragscode is een Financiële instelling gehouden interne instructies op te stellen en te geven waarin nader wordt aangegeven op welke wijze Persoonsgegevens door de Financiële instelling worden verwerkt. De interne instructies betreffen in ieder geval die onderwerpen waarvan de Financiële instelling van oordeel is dat nadere uitleg wenselijk is.

Bennet vraagt zich af of de controlerol wel voor de verantwoordelijke is weggelegd, of dat de controle beter kan worden gedaan door een onafhankelijke partij. "At this level, it is difficult to see how accountability of practice can be satisfactorily claimed without external and independent auditing".[574] Naar de mening van de Groep Gegevensbescherming Artikel 29 zou de controle op de naleving van de accountability plicht moeten worden uitgevoerd door de privacytoezichthouder. "Op verzoek van de privacytoezichthouders zouden verantwoordelijken moeten kunnen aantonen dat hun programma voldoet aan de eisen van

571 Bennet 2010, p. 7.
572 The Center for Information Policy Leadership 2009, p. 12.
573 Bruening, p. 3.
574 Bennet 2010, p. 7.

accountability".[575] In paragraaf 2.4 is echter de conclusie getrokken dat het Cbp niet snel tot handhaving op individueel niveau zal overgaan. Het is derhalve de vraag of het Cbp een actieve rol wil of kan gaan vervullen bij het toezicht houden op en handhaven van de accountability plicht. Interessant zou daarom zijn te bezien in hoeverre voor brancheorganisaties een rol kan zijn weggelegd bij het operationaliseren en (indirect) handhaven van de accountability plicht.[576]

Behalve de constatering dat de verantwoordelijke op grond van zijn accountability plicht adequate interne maatregelen moet treffen om gevolg te geven aan de bestaande beginselen voor gegevensbescherming en de doeltreffendheid van de waarborgen die hij daartoe implementeert, speelt accountability een relevante rol bij ondubbelzinnige toestemming. Zoals blijkt uit paragraaf 3.3 kan de betrokkene aan de hand van een privacyovereenkomst zijn ondubbelzinnige toestemming geven voor bepaalde verwerkingen. Met behulp van de geïmplementeerde maatregelen kan de verantwoordelijke aantonen (bewijzen) dat de betrokkene inderdaad daartoe zijn ondubbelzinnige toestemming heeft gegeven. *"Second*, in the context of a general accountability obligation, the controllers should be in a position to demonstrate that consent has been obtained. Indeed, if the burden of proof is reinforced so that data controllers are required to demonstrate that they have effectively obtained the consent of the data subject, they will be compelled to put in place standard practices and mechanisms to seek and prove unambiguous consent. The type of mechanisms will depend on the context and should take into account the facts and circumstances of the processing, more particularly its risks".[577]

De verhouding tussen transparantie enerzijds en accountability anderzijds is bij meerdere gelegenheden aan de orde gesteld. Naar de mening van de Groep Gegevensbescherming Artikel 29 versterkt transparantie de verantwoordingsplicht van de verantwoordelijke ten opzichte van de betrokkene.[578] De WRR stelt dat accountability aansluit bij de toetsbaarheid die door transparantie mogelijk wordt gemaakt, echter met toevoeging van bindende consequenties ('afrekening').[579] "In veel opzichten gaat transparantie dan ook vooraf aan accountability".[580] Ook in de kabinetsreactie op het WRR-rapport *i*Overheid wordt gerefereerd aan de verhouding tussen transparantie en accountability. "In de hieronder geschetste nieuwe beleidslijn trekt het kabinet deze transparantie door naar het op een geleidelijke en beheersbare wijze delen van gegevens met degene die het aangaat. Dit versterkt de aanspreekbaarheid (accountability) van diegenen die voor de

---

575 Groep Gegevensbescherming Artikel 29, Persbericht, 19 juli 2010.
576 In hoofdstuk 6 zal dit nader aan de orde komen.
577 Groep Gegevensbescherming Artikel 29-2011, p. 37.
578 Groep Gegevensbescherming Artikel 29-2010 (II), p. 16.
579 WRR rapport *i*Overheid, p. 84.
580 WRR rapport *i*Overheid, p. 84.

informatiehuishouding verantwoordelijk zijn".[581] Ook in de (buitenlandse) literatuur treffen we opvattingen aan over de verhouding tussen beide. Zo stellen Peng et al. dat accountability vereist dat de informatie transparant is. "Information accountability requires that the use of information should be transparent".[582] In ons land is ook Bovens deze mening toegedaan. "Organisational transparency and freedom of information will often be very important prerequisites for accountability, because they made provide forums with the necessary information".[583] In dat licht benadrukt Purtova dat een gebrek aan transparantie tot gevolg heeft dat verantwoording met betrekking tot inbreuken op gegevensverwerkingen een onbereikbaar doel wordt. "The lack of transparency in the data flow makes accountability for data protection violations a virtually unattainable goal. Firstly, the paths that personal data may take within the web of the data processing relationships are extremely entangled and difficult to trace or predict". "Secondly, within the multiplicity of the intertwined information chains, it is unclear how the burden of accountability for data protection is distributed among all of the involved actors, since their identity, as well as their exact contribution to the entire process, are not clear".[584] Kortom, transparantie is instrumenteel in het afleggen van verantwoording, en geeft daarmee handen en voeten aan accountability.[585]

5.6 Conclusies

Zoals ik hiervoor al opmerkte, is bij meerdere gelegenheden gewezen op het belang van zowel transparantie als accountability. De recente aandacht voor beide beginselen komt niet alleen voort uit allerhande maatschappelijke en technologische ontwikkelingen die normconforme persoonsgegevensbescherming onder druk zetten en daarmee tot meer handhaving door bevoegde instanties noodzaken. Ook de verantwoordelijke zelf wordt nu zeer expliciet door de (Europese) wetgever aangesproken meer verantwoordelijkheid te nemen voor 'law in action'.[586] Uit het voorstel van de Europese Commissie lijkt te kunnen worden opgemaakt dat zowel het transparantiebeginsel als het accountability beginsel zal worden geëxpliciteerd in de herziene Privacyrichtlijn.

De privacyverklaring lijkt in principe een werkbaar instrument om invulling te geven aan beide beginselen. Onderzoek in (met name) de Verenigde Staten laat echter zien dat, wil een privacyverklaring daadwerkelijk betekenis voor transparantie en accountability hebben, met de volgende aspecten rekening moet worden gehouden:

---

581 Kamerstukken II 2011-2012, 26643, nr. 211, p. 13.
582 Peng et al. p. 500.
583 Bovens, p. 13.
584 Purtova, p. 48.
585 Aldus Prins. Prins 2010, p. 7.
586 In hoofdstuk 1 (Inleiding) is uitgelegd wat onder 'law in action' wordt verstaan.

1. De naamgeving, traceerbaarheid en de toegankelijkheid van de privacyverklaring;
2. De vorm van de privacyverklaring; en
3. De inhoud, leesbaarheid en begrijpelijkheid van de privacyverklaring.

Het in hoofdstuk 4 gepresenteerde empirisch onderzoek laat zien dat het gebruik van privacyverklaringen niet eenduidig is. Indien de uitkomsten van het onderzoek worden vergeleken met de bovenstaande aspecten van transparantie, kan worden geconcludeerd dat de onderzochte privacyverklaringen niet de beoogde transparantie bieden.[587] Eerder uitgevoerd empirisch onderzoek naar het gebruik van privacyverklaringen in Nederland lijkt dit beeld te bevestigen. Dit heeft tevens tot gevolg dat de privacyverklaring zoals deze momenteel veelal in de praktijk wordt toegepast niet zal voldoen aan de maatstaf zoals die zal worden gesteld via het beginsel van accountability. Accountability vereist immers dat de informatie conform de voornoemde drie aspecten transparant is.

Wanneer de door mij geïdentificeerde aspecten van transparantie worden afgezet tegen onderzoek naar privacyverklaringen dat is uitgevoerd in de Verenigde Staten, stellen we vast dat deze aspecten niet of nauwelijks worden toegepast. Er is echter geen eenduidige conclusie te trekken wat exact de reden hiervoor is. Een mogelijke verklaring is dat er in de Verenigde Staten vanuit de overheid of private sectoren niet of nauwelijks wordt gestuurd op het gebruik van privacyverklaringen. Een voorbeeld waar wel op het gebruik van privacyverklaringen is gestuurd is de Gramm-Leach-Bliley Act.[588] Op grond van deze Act hebben financiële instituties in de Verenigde Staten de plicht om privacyverklaringen te presenteren aan hun klanten. Aanhakend bij deze verplichting is Kleimann een project gestart om een privacyverklaring te ontwikkelen ten behoeve van financiële instituties.

Het gebrek aan transparante privacyverklaringen heeft in de Verenigde Staten geleid tot de hypothese dat de gewenste mate van transparantie mogelijk kan worden gerealiseerd door het ontwikkelen van gestandaardiseerde privacyverklaringen. Ook de Europese Commissie overweegt in te zetten op het ontwikkelen van gestandaardiseerde privacyverklaringen. De Commissie heeft zich echter niet uitgelaten over de wijze waarop dit concreet gerealiseerd moet gaan worden, anders dan: “The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary”. De vraag is vervolgens welke verantwoordelijkheid de Europese Commissie en/of de Nederlandse wetgever op zich zouden moeten nemen ten aanzien van de ontwikkeling van gestandaardiseerde privacyverklaringen. In dit kader is tevens relevant de constatering dat het empirisch onderzoek in deze dissertatie aantoont dat sturing ten

[587] Er dient te worden opgemerkt dat de onderzochte privacyverklaringen niet zijn beoordeeld op de aspecten ‘leesbaarheid’ en ‘begrijpelijkheid’.

[588] Zie paragraaf 5.4.

aanzien van het gebruik van privacyverklaringen op brancheniveau effect lijkt te sorteren. Vanuit deze constatering bezien kan de vraag worden opgeworpen of brancheorganisaties een rol toebedeeld zouden moeten krijgen bij het ontwikkelen van gestandaardiseerde privacyverklaringen. In het volgende hoofdstuk zal daarom worden onderzocht welke rol (geconditioneerde) zelfregulering kan spelen ten aanzien van het ontwikkelen en gebruik van gestandaardiseerde privacyverklaringen, en wat de juridische status is van dergelijke zelfregulering.

Hoofdstuk 6 | De privacyverklaring als zelfreguleringsinstrument

6.1 Inleiding

Het empirisch onderzoek in deze dissertatie laat zien dat sturing op brancheniveau ten aanzien van het gebruik van privacyverklaringen effect sorteert. Onderzoek in de Verenigde Staten toont voorzichtig aan dat sturing door de wetgever op het gebruik van privacyverklaringen tevens effect lijkt te sorteren op de ontwikkeling (en mogelijk het gebruik) van privacyverklaringen. Ook de Europese Commissie overweegt hierin te gaan sturen. Kortom, sturing op het ontwikkelen en gebruik van gestandaardiseerde privacyverklaringen staat, redenerend vanuit transparantie en accountability, momenteel nadrukkelijk op de agenda. De vraag is dan natuurlijk op welke wijze deze sturing in de praktijk - EU-breed - moet worden vormgegeven. Daarbij dient enerzijds in ogenschouw te worden genomen dat het weinig effectief en efficiënt zou zijn als op lidstaatniveau gestandaardiseerde privacyverklaringen worden ontwikkeld. Anderzijds is juist binnen de lidstaten specifieke sectorale kennis voorhanden. Dit brengt mij op het vertrekpunt, namelijk dat waar het de ontwikkeling van een gestandaardiseerde privacyverklaring betreft, dit op hoofdlijnen op EU-niveau dient plaats te vinden, waarna de sectorale invulling daarvan op nationaal niveau gestalte kan krijgen. Vanuit dit vertrekpunt is in paragaaf 6.2 de vraag aan de orde of de ontwikkeling van de gestandaardiseerde privacyverklaring op hoofdlijnen op EU-niveau, alsook de sectorale invulling daarvan op nationaal niveau, moet plaatsvinden door sturing via overheids- dan wel zelfregulering. Kijkend naar een te prefereren keuze voor zelfregulering, wordt in paragraaf 6.3 vervolgens aandacht besteed aan enkele kenmerken en consequenties van sturing via zelfregulering. Tevens wordt onderzocht welke rol zelfregulering kan vervullen bij een nadere uitwerking van de informatieplicht, via het op brancheniveau ontwikkelen van gestandaardiseerde sectorale privacyverklaringen. Paragraaf 6.4 bevat tot slot aanbevelingen voor (het ontwikkelen van) gestandaardiseerde sectorale privacyverklaringen. Ook wordt in deze slotparagraaf het ambitieniveau beschreven dat ten aanzien van gestandaardiseerde sectorale privacyverklaringen nagestreefd zou moeten worden.

6.2 De keuze tussen overheidsregulering en zelfregulering

Wanneer we sturing op de ontwikkeling en het gebruik van gestandaardiseerde privacyverklaringen als uitgangspunt nemen, is de eerste vraag op welk niveau deze sturing plaats dient te vinden. Heeft de wetgever hier een rol te spelen of laten we het initiatief (vooralsnog) aan het veld zelf? Uit de literatuur kunnen diverse argumenten worden gedestilleerd die een eventuele keuze voor zelfregulering boven overheidsregulering

onderbouwen. Alvorens daar nader op in te gaan, sta ik allereerst kort stil bij het begrip zelfregulering. In de Nederlandse literatuur zijn diverse definities en omschrijvingen te vinden. Eijlander stelt dat zelfregulering betekent dat aan maatschappelijke organisaties bepaalde verantwoordelijkheden worden overgedragen of opgedragen in het kader van de regelgeving zelf of de uitvoering, controle en handhaving van die regelgeving.[589] Baarsma et al. menen dat zelfregulering inhoudt dat maatschappelijke partijen in bepaalde mate zelf verantwoordelijk zijn voor het opstellen en/of uitvoeren en/of handhaven van de regels.[590] Volgens Geelhoed is zelfregulering een vorm van bindende normstelling door een representatief kader uit de groep van belanghebbenden.[591] Van Driel definieert zelfregulering als niet-statelijke regels die al dan niet in samenwerking met anderen worden vastgesteld door degenen voor wie de regels bestemd zijn respectievelijk hun vertegenwoordigers, en waarbij het toezicht op de naleving mede door deze groepen wordt uitgeoefend.[592] Naar de mening van Witteveen is er sprake van zelfregulering als in een veld, domein of sector regels worden gemaakt, uitgevoerd en gehandhaafd door de direct betrokkenen of hun vertegenwoordigers.[593] Giesen spreekt van alternatieve regelgeving en wijst erop dat alternatieve regelgeving ook wel geduid of benoemd wordt als zelfregulering.[594] Hij benoemt een aantal kenmerken van zelfregulering. Het eerste kenmerk is dat alternatieve regelgeving of zelfregulering steeds tegenover overheidsregulering wordt geplaatst, en dat dan ook nog eens bij wijze van tegenstelling. “Ten tweede gaat het steeds om ‘privaatrechtelijke’ verschijnselen zodat ook het onderscheid publiek/privaatrecht een rol schijnt te spelen”. Wezenlijk is verder – als derde - dat het bij zelfregulering om een vorm van collectiviteit gaat. Ten vierde is het voor zelfregulering nog wezenlijk dat degene die reguleert, ook (zelf) gereguleerd wordt, aldus Giesen.[595]

Zoals gezegd, worden in de literatuur verschillende argumenten gepresenteerd die een eventuele keuze voor zelfregulering boven overheidsregulering onderbouwen. De Nota Wes (Nota Wetgeving voor de Elektronische Snelweg) stelt dat die voorkeur kan worden beargumenteerd vanuit de gedachte dat in een zich snel wijzigende en technisch complexe en internationale omgeving maatschappelijke partijen soms over meer expertise en inzicht in

589 Eijlander 1993, p. 181.

590 Baarsma et al., p. 13.

591 Geelhoed, p 49.

592 Van Driel, p. 2. Zij stelt dat bij zelfregulering in zekere zin geldt: normsteller = normadressaat = toezichtverantwoordelijke.

593 Witteveen, p. 29. Het reguleringsspectrum van Witteveen omvat ‘Regulering – Alternatieve regulering – Zelfregulering – Non-regulering’, Witteveen p. 23 e.v. Zie in dit kader de bijdragen van Prins, Van der Vlies, Hartlief en Buruma in *NJB* 2007, 21, welk nummer in het teken staat van de preadviezen voor de NJV-Vergadering over Alternatieve regelgeving.

594 “De brede term alternatieve regelgeving sluit in wezen weinig uit, en omvat daarmee eigenlijk alle regelgeving (algemeen en herhaaldelijke toepasbare (gedrags)normen) die niet als ‘gewone’ regelgeving is te kwalificeren, dus: alternatieve regulering, zelfregulering en non-regulering”. Giesen 2007-b, p. 7.

595 Giesen 2007-b, p. 9 e.v.

de aard van de problemen en de haalbaarheid en adequaatheid van mogelijke oplossingen beschikken, dan een relatieve buitenstaander als de overheid.[596] Teunissen wijst erop dat zelfregulering in de eigen particuliere kring in het Nederlands privaatrecht al heel oude papieren heeft, en dat de maatschappelijke betekenis van deze zelfregulering enorm is.[597] Overigens merkt hij daarbij op dat, waar wordt ingezet op zelfregulering, gewaakt moet worden tegen het vervagen van het fundamentele onderscheid tussen de publieke en de private sfeer. “Maatschappelijke en belangenorganisaties zijn geen onderdeel van de Staat. Waar ze overgaan tot zelfregulering, doen ze dit – óók als die zelfregulering is geconditioneerd door overheidsregelgeving – ter behartiging van het groepsbelang en niet ter verwezenlijking van publieke doelen. Dat neemt niet weg dat groepsbelangen parallel kunnen lopen met publieke belangen en dat bijgevolg door (de wijze van) zelfregulering ook publieke belangen kunnen worden gediend”.[598] Vranken komt tot de conclusie dat meer en meer private regelgeving wordt geaccepteerd en door de wetgever zelfs welbewust wordt bevorderd.[599] Tevens wijst hij op de beperkingen van overheidsregulering, en stelt dat wetgeving kan worden beschouwd als het geven van algemene normen voor rechtsrelaties tussen rechtssubjecten.[600] “Regels kunnen naar hun aard niet anders dan tot op zekere hoogte abstract, algemeen en, zo men wil, vaag (open) zijn. Zij zijn erop gericht een diversiteit van situaties te bestrijken. Dat kan alleen wanneer men aangeeft wat deze situaties gemeenschappelijk hebben, dit wil zeggen door te abstraheren van alle details die niet ter zake doen”.[601] “Tevens kan een codificatie nooit uitputtend of volledig zijn, niet op het moment van totstandkoming ervan en zeker niet na verloop van enige tijd als nieuwe ontwikkelingen beginnen te wringen met de in de codificatie gemaakte keuzen”.[602] Vranken komt tot de conclusie dat wetgeving en rechtspraak, ook in combinatie met opvattingen in de literatuur, er samen niet in slagen de behoefte aan voldoende en duidelijke regels in het burgerlijk recht te dekken.[603] “De reden hiervoor is dat ‘de’ maatschappelijke werkelijkheid waarop het burgerlijk recht betrekking heeft, voortdurend in beweging is”.[604] Ook uit de Aanwijzingen voor regelgeving kan worden opgemaakt dat zelfregulering in bepaalde situaties wordt geacht een goed alternatief voor overheidsregulering te zijn. Zo volgt uit aanwijzingnummer 7 sub c dat, alvorens tot het treffen van een regeling wordt besloten, onderzocht moet worden of de gekozen doelstellingen kunnen worden bereikt door middel van het zelfregulerend vermogen in de betrokken sector (sectoren) dan wel door overheidsinterventie. Naast de hiervoor door Vranken genoemde nadelen van

596 Nota Wes, pag. 180.
597 Teunissen, p. 8.
598 Teunissen, p. 11.
599 Vranken 2004-a, p. 5.
600 Vranken 2004-b, p. 52 e.v.
601 Vranken 2004-a, p. 3.
602 Vranken 2004-b, p. 54.
603 Vranken 2004-a, p. 11.
604 Vranken 2004-a, p. 11.

overheidsregulering, biedt sturing op dit niveau ook voordelen. Overheidsregulering geeft rechtszekerheid, waarborgt fundamentele waarden, plichten en belangen in de rechtstaat en beschermt de (nationale) concurrentiepositie.[605] Eijlander en Voermans noemen als kracht van overheidsregulering: rechtsgeldigheid, bekendheid, acceptatie en legitimatie en nalevingsbereidheid.[606]

De voordelen van zelfregulering die Baarsma et al. schetsen, zien onder meer op flexibiliteit, verlichting van het overheidsapparaat en betrokkenheid van de samenleving. De nadelen betreffen onder andere het gevaar voor misbruik van een informatievoorsprong, beperkte afdwingbaarheid van regels en het gevaar voor lobbygroepen.[607] Giesen benadrukt dat aan zelfregulering gevaren zitten als 'corporatism' en doelt daarmee op het verkrijgen van (teveel) macht door groepen die vervolgens geen verantwoording schuldig zijn aan het publiek langs de gebruikelijke politieke kanalen.[608] Eijlander en Voermans komen tot het volgende overzicht met betrekking tot de voor- en nadelen van zelfregulering:[609]

De voordelen en nadelen van zelfregulering volgens Eijlander en Voermans	
Voordelen	**Nadelen**
• betere aansluiting van de regels op het handelingsperspectief van de betrokkenen; • grotere bereidheid tot naleving van de zelfgestelde regels; • geringere uitvoeringslasten voor de overheid; • nauwere band tussen het nemen van beslissingen en het dragen van de gevolgen daarvan; • grotere betrokkenheid van burgers en maatschappelijke organisaties bij het desbetreffende onderwerp, vanwege de toegenomen mogelijkheid om zelf in ruimere mate richting te geven aan het gedrag.	• toenemende macht van de sterkste of de best georganiseerde; • mogelijk beperkte doordringbaarheid van de zelfreguleringscollectiviteit of –instantie voor geluiden of impulsen uit de buitenwereld; • daling van het niveau van regulering; • beperkte afdwingbaarheid van de (groeps)regels; • (soms) onnodige verschillen in regelgeving; • toenemende uitvoeringslasten voor burgers en maatschappelijke organisaties.

Tabel 6.1

605 Wagemans, p. 63 en Witteveen, p. 26.
606 Eijlander & Voermans, p. 19 e.v.
607 Baarsma et al., p. 21.
608 Giesen 2007-a, p. 86.
609 Eijlander & Voermans, p. 75.

Zelfregulering dient aan een aantal elementaire voorwaarden te voldoen, wil het als een aanvaardbaar alternatief voor overheidsregulering worden beschouwd.[610] Deze voorwaarden zijn:

1. De doelgroepen die in het geding zijn, zijn voldoende georganiseerd;
2. Er vindt een gelijkwaardige behartiging van de maatschappelijke belangen plaats;
3. Er vindt voldoende binding plaats van alle partijen; en
4. De handhaving van de afspraken is voldoende verzekerd.

Koops et al. onderscheiden een aantal criteria dat in acht dient te worden genomen bij een keuze tussen overheids- en zelfregulering.[611]

Eerlijkheid: Eerlijkheid houdt in dat de sociale belangen van zwakkere partijen voldoende gewaarborgd moeten worden.[612] "Fairness is one of the prime indicators for government involvement. If fundamental rights are at stake or if certain groups threaten to be discriminated, self-regulation is not an adequate instrument".[613]

Representativiteit: Het proces waarlangs het zelfreguleringsinitiatief tot stand komt dient voldoende representatief te zijn. "Daarmee wordt met name gedoeld op de representativiteit van degene die de regels opstelt voor de adressaten van de zelfregulering".[614] "For self-regulation to work, the stakeholders should be well organized in order to ensure that the people participating in the process know the needs and desires of their colleagues and the people they represent".[615]

Toezicht en naleving: De naleving van zelfregulering en de handhaving daarvan door middel van toezicht, is een belangrijke voorwaarde voor de effectiviteit van zelfregulering. "Van belang hiervoor is de mate waarin en de instrumenten waarmee organisaties die onder de zelfregulering vallen aansprakelijk kunnen worden gehouden voor het niet naleven van de regels waarvan de consument mag verwachten dat zij die nakomen".[616] "For if an organization lacks the means, power, and authority to enforce its norms, then their value remains symbolic. Thus, a convincing case for self-regulation can only be made if the relevant parties to the self-imposed rules or standards formulate organizational compliance measures with inherently binding provisions, for example, in operational policies".[617] Baarsma et al. wijzen erop dat onduidelijkheid over toezicht, controlemaatregelen en

---

610 Teunissen, p. 10.

611 Koops et al., p. 136 e.v. Nouwt heeft deze criteria vertaald naar het Nederlands, en aangevuld met het criterium 'continuïteit'. Nouwt 2005, p. 113 e.v. Ook Holvast & Gardeniers hebben afwegingen en voorwaarden gedefinieerd met betrekking tot een set zelfreguleringsafspraken en het stelsel voor het vaststellen, de herziening en toepassing van deze afspraken. Holvast & Gardeniers, p. 66 e.v. Zie ook Van Driel die een leidraad voor zelfregulering heeft opgesteld. Van Driel, p. 120 e.v.

612 Nouwt 2005, p. 113.

613 Koops et al., p. 136.

614 Nouwt 2005, p. 113.

615 Koops et al., p. 136.

616 Nouwt 2005, p. 114.

617 Koops et al., p. 137 e.v.

sancties de slaagkans van het instrument zelfregulering ernstig bemoeilijken.[618] Het kabinet definieert toezicht als volgt: “Toezicht is het verzamelen van de informatie over de vraag of een handeling of zaak voldoet aan de daaraan gestelde eisen, het zich daarna vormen van een oordeel daarover en het eventueel naar aanleiding daarvan interveniëren”.[619] Giesen concludeert dat een toezichthouder drie taken heeft, te weten: informatie verzamelen (ofwel: kennis vergaren), een oordeel vormen en zo nodig ingrijpen.[620]

Transparantie: Hiermee wordt bedoeld dat de regels met betrekking tot het zelfreguleringsinitiatief kenbaar en duidelijk moeten zijn, maar ook de wijze van totstandkoming van het initiatief.[621] “Contrary to (the theory of) democratic rule-making, self-regulation may be an obscure and behind-the-scene process. If the people affected by self-regulation are not made aware of the process, they cannot try and influence it to their benefit; and if the resulting rules are invisible or untransparent, they cannot complain if they are adversely affected”.[622]

Rechtszekerheid: “Bij rechtszekerheid draait het om de vraag of de regels wel voldoende duidelijk zijn, ondubbelzinnig en consistent”.[623] “However, it is not easy to say wether legal certainty in general is an argument for or against self-regulation. In some cases, self-regulation is better suited to provide legal certainty, for instance, if the field is rapidly changing and flexibility in updating rules is called for”.[624]

Context: “Van belang voor de effectiviteit van zelfregulering is de context waarbinnen zelfregulering wordt ontwikkeld”. De context wordt mede bepaald door de branche, het domein of voorwerp van de zelfregulering, de techniek die wordt gebruikt en of de zelfregulering op nationaal of internationaal niveau wordt ontwikkeld.[625]

Efficiëntie: Zelfregulering is veelal flexibeler dan overheidsregulering. Daardoor is zelfregulering makkelijker aan te passen in veranderende omstandigheden.[626] “Government regulation is often regarded as cumbersome, timeconsuming, and costly, while self-regulation is more flexible and therefore better suited for regular updating with developments”.[627]

Continuïteit: “Daarmee wordt in het bijzonder gedoeld op de continuïteit van het zelfreguleringsinitiatief of van de organisatie die het zelfreguleringsinitiatief heeft opgezet”.[628]

---

618 Baarsma et al., p. 31.
619 Kamerstukken II 2000/01, 27 831, nr. 1.
620 Giesen 2005, p. 20.
621 Nouwt 2005, p. 114.
622 Koops et al., p. 138.
623 Nouwt 2005, p. 114.
624 Koops et al., p. 138.
625 Nouwt 2005, p. 115.
626 Nouwt 2005, p. 115.
627 Koops et al., p. 139.
628 Nouwt 2005, p. 115.

Kijkend naar het gewenste niveau van sturing, moet ook worden stilgestaan bij de traditie op het terrein van gegevensbescherming waar het de inzet van instrumenten betreft die de wettelijke bepalingen van de Wbp nader uitwerken. Binnen deze traditie lijkt zelfregulering (in instantie) de voorkeur te genieten. Zo werd al in de juridische en sociaalwetenschappelijke evaluaties van de Wet persoonsregistratie (de voorloper van de Wbp) geconcludeerd dat zelfregulering bij de nadere uitwerking van de wettelijke bepalingen de voorkeur geniet boven overheidsregulering. Toentertijd werd in het bijzonder gedoeld op de totstandkoming van sectorale gedragscodes, die onder het regime van de Wpr als instrument werden ingezet.[629] Deze zienswijze is bevestigd in de Privacyrichtlijn, waarin wordt benadrukt dat lidstaten beroepsgroepen moeten aanmoedigen gedragscodes op te stellen.[630] De MvT omschrijft de Wbp als een abstract normenkader dat door middel van sectorale wetgeving of zelfregulering verdere invulling zal moeten krijgen. “Organisaties kunnen er voor kiezen zelf in een gedragscode een nadere invulling te geven aan het normenkader van de Wbp”.[631] Naar de mening van Giesen wordt bij regulering van privacy het instrument van zelfregulering ook daadwerkelijk benut. “Het recht inzake privacy is geregeld in de Wbp, maar evenzeer of wellicht zelfs meer nog in de diverse uitwerkingen daarvan via bijvoorbeeld overeenkomsten (modelclausules van de Internationale Chamber of Commerce), aanbevelingen (van de OECD), gedragscodes (al dan niet voorzien van het ‘keurmerk’ van het Cbp zoals bedoeld in art. 25 Wbp) en algemene privacystatements”.[632] In de internationale literatuur stelt Raab dat zelfregulering in relatie tot de verwerking van persoonsgegevens zich heeft ontwikkeld tot “a variety of tools that include privacy commitments, codes of practice, adherence to standards, and online tokens or seals”.[633]

Ook de toezichthouder heeft in het verleden het belang van zelfregulering onderstreept. Zo refereert het Cbp in het kader van de informatieplicht aan het instrument van zelfregulering, omdat de verantwoordelijke langs deze weg beter, sneller en effectiever aan die informatieplicht kan voldoen.[634] Wat betreft de positie van de wetgever, stellen we vast dat volgens het kabinet Balkenende IV zelfregulering in belangrijke mate bijdraagt aan een correcte omgang met persoonsgegevens. “Het bevorderen van zelfregulering vormt dan ook een onderdeel van de benadering van het kabinet, wanneer het gaat om de verwerking van persoonsgegevens buiten het veiligheidsdomein. Het erop toezien dat persoonsgegevens op een behoorlijke manier worden verwerkt, is immers niet primair een zaak van de

629 Zie voor de juridische evaluatie Overkleeft-Verburg en voor de sociaal-wetenschappelijke evaluatie Prins et al.
630 Overweging (61) en artikel 27 van de Privacyrichtlijn.
631 Kamerstukken II 1997-1998, 25892, nr. 3, p. 16.
632 Giesen 2007-b, p. 26.
633 Raab, p. 9.
634 Holvast, p. 116.

toezichthouder".[635] Ook wijst dit kabinet Balkenende op de mogelijkheden die de Wbp biedt tot sectorgewijze invulling van de regelgeving door middel van gedragscodes, alsook de optie dat bedrijven of instellingen kunnen besluiten tot de aanstelling van een functionaris voor de gegevensbescherming. "Burgers en bedrijven moeten zoveel mogelijk vrijheid worden gegund bij de wijze waarop zij invulling geven aan een gecompliceerde wet".[636] Het kabinet Balkenende IV ziet meer in het door middel van wetgeving stimuleren van het gebruik van deze instrumenten.[637] Meer recent stelt het kabinet Rutte in de Notitie Privacybeleid van april 2011, dat de gegevensbescherming veel kan winnen wanneer het bedrijfsleven in staat en bereid is volgens de weg van een zo groot mogelijke mate van zelfregulering privacybescherming tot normaal onderdeel van het ondernemingsbeleid te maken.[638] Ook in het debat met betrekking tot wijziging van de Telecommunicatiewet refereert het kabinet Rutte aan zelfregulering. "Zelfregulering heeft de voorkeur boven wetgeving vanwege de wens om de administratieve lasten voor bedrijven tot een minimum te beperken. Een rol voor de overheid ontstaat als consumenten collectief problemen van structurele aard tegenkomen, die door de markt onvoldoende worden opgelost".[639]

Kijken we naar de dagelijkse realiteit, dan stellen we vast dat ondanks het vertrouwen van diverse actoren in het instrument van zelfregulering, het succes daarvan in relatie tot de bescherming van persoonsgegevens vooralsnog beperkt is. Zwenne et al. concluderen dat in de publieke sector relatief veel FG's zijn aangesteld, maar dat er niet of nauwelijks sprake is van sturing via een instrument als gedragscodes.[640] Daarmee laat zelfregulering in het kader van de Wbp te wensen over, aldus Zwenne et al.[641] De reden waarom de gedragscodes, zoals bedoeld in artikel 25 Wbp, niet van de grond komen is mede gelegen in de tijdrovende goedkeuringsprocedure die bij het Cbp moet worden doorlopen, waardoor vaak van goedkeuring wordt afgezien.[642] Ook op Europees niveau zijn nauwelijks communautaire gedragscodes, zoals bedoeld in artikel 27 lid 3 Privacyrichtlijn, tot stand gekomen.[643] Nouwt stelt in dit kader dat op Europees niveau weinig interesse bestaat voor zelfregulering in relatie tot de bescherming van persoonsgegevens. "This indicates that there is very little interest for self-regulation of data protection at a European level".[644]

---

635 Kamerstukken II 2009–2010, 31051, nr. 5, p. 29.

636 Kamerstukken II 2009–2010, 31051, nr. 5, p. 29.

637 Kamerstukken II 2009–2010, 31051, nr. 5, p. 29.

638 Kamerstukken II 2010-2011, 32761, nr. 1, p. 11.

639 Kamerstukken II 2010-2011, 32549, nr. 7, p. 10.

640 Zwenne et al., p. 12.

641 Zwenne et al., p. 13.

642 Winter et al., p. 148.

643 Een voorbeeld van een Europese gedragscode betreft die van The Federation of European and Interactive Marketing (FEDMA).

644 Nouwt 2009, p. 284. Op internationaal niveau lijkt het zelfreguleringsinitiatief van multinationals met betrekking tot Binding Corporate Rules meer succesvol te zijn. Zie Moerel, p. 271 e.v.

Wat betekent het voorgaande concreet voor de ontwikkeling van gestandaardiseerde sectorale privacyverklaringen? In dit kader is het relevant te kijken naar het, eerder aangehaalde, voorstel van de Europese Commissie (2012) waaruit lijkt te kunnen worden opgemaakt dat de Commissie overweegt gestandaardiseerde privacyverklaringen vast te stellen of voor te schrijven: “The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)”.[645] Uit de tekst wordt niet duidelijk of de Europese Commissie zelf gestandaardiseerde sectorale privacyverklaringen wil ontwikkelen, of dat zij het initiatief daartoe wil overlaten aan de markt. Naar mijn interpretatie houdt de Europese Commissie de weg vrij voor een keuze tussen overheids- of zelfregulering, en tracht de Commissie vooraleerst de markt te bewegen gestandaardiseerde sectorale privacyverklaringen te ontwikkelen en te gebruiken, onder ‘dreiging’ het zelf te zullen doen. In dat laatste geval lijkt het mij voorstelbaar dat een gebruik van gestandaardiseerde sectorale privacyverklaringen wettelijk zal worden afgedwongen.[646]

In de inleiding tot dit hoofdstuk is als vertrekpunt genomen dat een gestandaardiseerde privacyverklaring op hoofdlijnen op EU-niveau moet worden ontwikkeld, en de sectorale invulling daarvan op nationaal niveau moet plaatsvinden. Uit de voorgaande bespreking over overheids- en zelfregulering, zijn drie argumenten te destilleren die ervoor pleiten de - op EU-niveau - te ontwikkelen gestandaardiseerde privacyverklaring op hoofdlijnen tot stand te laten komen door sturing door middel van overheidsregulering. Ten eerste valt een keuze voor zelfregulering boven overheidsregulering in het algemeen te overwegen indien specifieke sectorale kennis, flexibiliteit en maatschappelijke betrokkenheid noodzakelijk is. Met betrekking tot de te ontwikkelen gestandaardiseerde privacyverklaring op hoofdlijnen lijken deze aspecten niet van een dusdanige relevantie dat dit een voorkeur voor zelfregulering boven overheidsregulering zou staven. Ten tweede speelt representativiteit, of beter gezegd het mogelijk ontbreken daarvan, een rol. De groep van belanghebbenden lijkt niet eenvoudig te kunnen worden bepaald. Daar komt bij dat die groep voldoende georganiseerd dient te zijn wil het betekenis krijgen voor zelfregulering. Dit geldt evenzo voor de gesprekspartner(s) van die groep van belanghebbenden, die ervoor moet zorgdragen dat een gelijkwaardige behartiging van de maatschappelijke belangen wordt gewaarborgd. Ten derde is gebleken dat zelfregulering op EU-niveau vooralsnog weinig

645 Artikel 14 lid 8 COM (2012) 11 final.

646 Op grond van artikel 14 lid 8 COM (2012) 11 final juncto artikel 87 lid 2 COM (2012) 11 final juncto artikel 5 Verordening 182/2011. Verordening (EU) Nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren.

succesvol is gebleken. Kortom, de Europese Commissie zou het initiatief naar zich toe moeten trekken om een gestandaardiseerde privacyverklaring op hoofdlijnen te ontwikkelen.[647] Dit wil overigens niet zeggen dat belanghebbenden geen inspraak zouden moeten hebben bij die ontwikkeling. Marktpartijen en overige belanghebbenden zouden aan de hand van publieke consultaties in staat moeten worden gesteld visies en aanbevelingen te delen met de Europese Commissie.[648]

Vervolgens is de vraag aan de orde of de nadere sectorale invulling van de gestandaardiseerde privacyverklaring op nationaal niveau door sturing via overheidsregulering dan wel zelfregulering dient plaats te vinden. Op grond van de voorgaande bespreking over overheids- en zelfregulering, pleit een aantal argumenten voor een nadere sectorale invulling via zelfregulering. Ten eerste lijkt de Europese Commissie, zoals hiervoor besproken, aan te sturen op zelfregulering. Ten tweede is voor de nadere invulling specifieke sectorale kennis benodigd; kennis die voornamelijk aanwezig zal zijn bij brancheorganisaties. Ook aspecten als flexibiliteit, maatschappelijke betrokkenheid en een grotere mate van bereidheid tot naleving van de zelfgestelde regels, ondersteunen een keuze voor zelfregulering boven overheidsregulering. Ten derde laat het empirisch onderzoek in deze dissertatie zien dat een sturend optreden op brancheniveau effect sorteert waar het de privacyverklaring betreft. Ten vierde lijkt het niet wenselijk dat de wettelijke informatieplicht 'in detail' wordt uitgewerkt; de Privacyrichtlijn en de Wbp (artikelen 33 en 34 Wbp) werken met een stelsel van open normen en zouden met een nadere uitwerking specifiek voor de privacyverklaring sterk van karakter veranderen.[649] Het laatste argument dat pleit voor zelfregulering op nationaal niveau is gelegen in het feit dat een aantal relevante actoren (waaronder het Cbp) naar verwachting, althans in Nederland, geen initiatieven zal ondernemen. Het Cbp stelt zich op het standpunt dat een actievere invulling van de transparantieverplichting gerealiseerd kan worden met behulp van privacystatements.[650] Uit onderzoek van Winter et al. blijkt echter dat het Cbp in het verleden geen 'ontwikkelende' en stimulerende rol heeft vervuld bij de totstandkoming van

---

647 Vergelijk in dit verband de 'EU Standard Contractual Clauses' die de Europese Commissie heeft opgesteld in het kader van doorgifte van persoonsgegevens naar verwerkers die in derde landen zijn gevestigd. Besluit van de Commissie betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG van het Europees Parlement en de Raad, Brussel, 5.2.2010, C(2010)593 definitief. Zie Moerel p. 210.

648 Voorbeelden van public consultations betreffen de "Consultation on the Commission's comprehensive approach on personal data protection in the European Union" en "Consultation on the future European Union (EU) - United States of America (US) international agreement on personal data protection and information sharing for law enforcement purposes".

649 Ook artikel 8 lid 1 sub h. COM (2012) 11 final kent open normen: "Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: (h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected".

650 Cbp, Jaarverslag 2009, p. 49.

sectorale regelgeving en/of gedragscodes.[651] "De respondenten die wij in het kader van het onderzoek hebben gesproken menen dat van een sterk stimulerende rol van het Cbp met het oog op de normontwikkeling niet kan worden gesproken."[652] De te verwachten terughoudende opstelling van het Cbp kan ook worden afgeleid uit het feit dat de in 2009 aangekondigde "Richtsnoeren inzake de informatieplicht" tot op heden nog niet is verschenen.[653] Deze houding van het Cbp valt te verklaren vanuit de verschuiving in prioriteiten, namelijk naar het doen van onderzoek en het handhavend optreden.[654] Kijkend naar een eventuele initiërende rol van het kabinet, kan worden vastgesteld dat deze in beginsel het gebruik van EU-brede privacyverklaringen ondersteunt. Het is echter weinig realistisch te verwachten dat de regering met betrekking tot het ontwikkelen van gestandaardiseerde privacyverklaringen een actieve rol zal vervullen, aangezien het zich bij meerdere gelegenheden heeft uitgelaten voorkeur te geven aan zelfregulering boven overheidsregulering.[655] Wel zal de overheid een voorbeeldfunctie kunnen vervullen waar het gaat om het gebruik van een op te stellen gestandaardiseerde verklaring en daarmee *best practices* binnen de publieke sector.

6.3 De gestandaardiseerde sectorale privacyverklaring als zelfreguleringsinstrument

In de voorgaande hoofdstukken is gesproken over de informatieplicht uit de Wbp die de verantwoordelijke jegens de betrokkene in acht dient te nemen indien hij diensten of producten exploiteert via zijn website. Daarbij is duidelijk geworden dat de verantwoordelijke, op grond van de open normen uit de artikelen 33 en 34 Wbp, zelf de informatieplicht nader moet invullen. In geval van zelfregulering kan de nadere invulling van de informatieplicht op brancheniveau worden vastgesteld. In dit onderzoek ziet de zelfregulering derhalve op een nadere uitwerking van de informatieplicht op brancheniveau, waarbij de brancheorganisaties zorg beogen te dragen voor een nadere sectorale invulling van de gestandaardiseerde privacyverklaringen die op hoofdlijnen door de Europese Commissie wordt ontwikkeld. De gestandaardiseerde sectorale privacyverklaring is te kwalificeren als zelfreguleringsinstrument.[656] Het proces vanaf initiatie tot aan de

---

651 Winter et al., p. 147.

652 Winter et al., p. 148.

653 Cbp Jaarverslag 2009, p. 10.

654 Zie ook paragraaf 2.4.1.

655 Zie paragraaf 6.2.

656 Baarsma et al. hebben 22 zelfreguleringsinstrumenten geïdentificeerd. Deze instrumenten zijn door hen vanuit het oogpunt van de gebruikers in vijf verschillende clusters ingedeeld, te weten techniekgerichte instrumenten, gedragsgerichte instrumenten, informerende instrumenten, contractuele instrumenten en geschilbeslechtende instrumenten. Daarnaast onderscheiden zij publiekrechtelijke beroepsorganisaties, die volgens hen een zeer vergaande vorm van zelfregulering is. Baarsma et al., p. 23. Het is overigens opvallend dat Baarsma et al. een privacyverklaring niet noemt als zelfreguleringsinstrument, terwijl in veel andere literatuur een

totstandkoming van de zelfregulering wordt in dit onderzoek aangeduid als zelfreguleringsinitiatief.
Wat de implicaties van de zelfregulering kunnen zijn als het aankomt op nadere sturing met betrekking tot het opstellen en gebruik van gestandaardiseerde sectorale privacyverklaringen, zal in het navolgende worden bezien.

6.3.1 De informatieplicht uit de Wbp: wettelijk geconditioneerde zelfregulering

Zelfregulering kent verschillende gedaanten. Giesen onderscheidt eenzijdig of tweezijdig tot stand gekomen zelfregulering. “Bij eenzijdige zelfregulering is een deel van de betrokkenen die door de zelfreguleerder gebonden wordt niet betrokken geweest bij het opstellen van de regels. Bij tweezijdige zelfregulering is dat wel het geval”.[657] Naar de mening van Van Driel is er sprake van eenzijdige zelfregulering indien alleen het bedrijfsleven is betrokken. In de gevallen dat groepen die de andere kant van de markt vertegenwoordigen tevens betrokken zijn, is er volgens Van Driel sprake van twee- of meerzijdige zelfregulering.[658] In de literatuur wordt veelal verwezen naar Eijlander die zelfregulering onderscheidt in 3 typen.[659] Het eerste type betreft de zuivere vorm van zelfregulering. Kenmerkend hierbij is dat het initiatief ligt bij de belanghebbenden; de overheid heeft geen sturende of initiërende rol en stelt zich neutraal op tegenover de inhoud van de overeengekomen regels, zolang zij niet in strijd zijn met algemeen geldende rechtsregels. Het tweede type betreft de vorm van zelfregulering waarbij de overheid drang uitoefent om tot zelfregulering te komen, echter zonder dat hier een uitdrukkelijke verplichting aan ten grondslag ligt (in de literatuur wordt dit betiteld als vervangende zelfregulering). Ook in deze vorm wordt door de overheid het initiatief overgelaten aan de belanghebbenden, maar zij behoudt zich het recht voor om zelf met wetgeving te komen indien de belangen niet of onvoldoende door de in eigen beheer vastgestelde normen worden beschermd. Voornoemde typen van zelfregulering hebben gemeen dat ze niet binnen een wettelijk kader tot stand zijn gekomen. De vorm van zelfregulering die binnen een wettelijk kader tot stand komt wordt aangeduid als wettelijk geconditioneerde zelfregulering. Volgens Eijlander is het kenmerk van wettelijk geconditioneerde zelfregulering dat de wetgever zich beperkt tot het stellen van enige (materiële of procedurele) randvoorwaarden, de belanghebbenden een aanzienlijke vrijheid hebben bij de invulling van het wettelijke kader en dat de overheid een voorname plaats heeft bij de controle op het eindresultaat.[660] Tevens betoogt Eijlander dat de wijze en mate van conditionering van zelfregulering uiteen lopen. Hij verduidelijkt zijn stelling met

---

privacyverklaring wel als zodanig wordt aangemerkt. Zie in dit kader Koops et al., p. 127; Bennet 2004, p. 230; Bendrath, p. 196 en Giesen 2007-b, p. 26.

657 Giesen 2007-b, p. 15.

658 Van Driel, p. 12.

659 Eijlander 1994, pag. 100 e.v. Voor verwijzingen naar het door Eijlander gemaakte onderscheid in 3 typen zelfregulering zie onder andere Geelhoed, pag. 49 e.v., Giesen 2007-b, p. 14 e.v., Teunissen, p. 8 e.v. en Witteveen, p. 30 e.v.

660 Eijlander 1994, pag. 101.

praktijkvoorbeelden waarbij de wetgever enerzijds volstaat met het aangeven van de procedure van totstandkoming van de zelfregulering en waarbij de wetgever anderzijds zodanige inhoudelijke randvoorwaarden stelt dat nauwelijks meer van zelfregulering kan worden gesproken.[661] Geelhoed vult daarbij aan dat de overheid duidelijke randvoorwaarden stelt aan het door de belanghebbenden te bereiken resultaat en merkt op dat de wettelijk geconditioneerde vorm van zelfregulering en de publieke normstelling complementair aan elkaar zijn.[662]

Op basis van het voorgaande kunnen de typen van zelfregulering en de bijhorende kenmerken als volgt worden weergegeven:

Overzicht typen van zelfregulering volgens Eijlander			
Type	**Initiatiefnemer**	**Wettelijk kader**	**Participatie van de overheid**
Zuivere zelfregulering	Belanghebbenden	Nee	Neutraal. De overheid onderneemt geen actie indien de afspraken niet in strijd zijn met algemeen geldende rechtsregels
Vervangende zelfregulering	Belanghebbenden. De overheid oefent drang uit om tot zelfregulering te komen (er ligt echter geen verplichting aan ten grondslag)	Nee	De overheid behoudt zich het recht voor om zelf met wetgeving te komen indien de belangen niet of onvoldoende worden beschermd door de in eigen beheer vastgestelde normen
Wettelijk geconditioneerde zelfregulering	Belanghebbenden	Ja	De overheid stelt de wettelijke kaders vast waarbinnen de zelfregulering kan plaatsvinden

Tabel 6.2

In dit onderzoek is meerdere keren aan de orde gekomen dat op grond van de informatieplicht, zoals neergelegd in de artikelen 33 en 34 Wbp, de betrokkene geïnformeerd dient te worden over de identiteit van de verantwoordelijke en het doel van de verwerking. De Wbp schrijft niet concreet voor op welke wijze aan de informatieverplichting moet worden voldaan, en wat de aanduiding ‘nadere informatie’ dient te omvatten. De wetgever schetst daarmee een relatief open wettelijk kader van de informatieplicht en geeft ruimte om binnen dit kader de uitwerking naar eigen inzicht in te vullen, op uitdrukkelijke

661 Eijlander 1994, pag. 102.
662 Geelhoed, pag. 49 e.v.

voorwaarde dat die informatie wordt verstrekt voor zover dat nodig is gelet op (i) de aard van de gegevens, (ii) de omstandigheden waaronder de gegevens worden verkregen en (iii) het gebruik dat van de gegevens wordt gemaakt. De zelfregulering die op grond van het zelfreguleringsinitiatief tot stand komt wordt, op basis van de door Eijlander onderscheiden typen zelfregulering, gekwalificeerd als wettelijk geconditioneerde zelfregulering. In geval van wettelijk geconditioneerde zelfregulering laat de overheid het initiatief aan de markt, maar stelt zij aan het te bereiken resultaat duidelijke randvoorwaarden, die soms expliciet in een wettelijke regeling vastgelegd kunnen zijn.[663] In het huidige wettelijk kader van de informatieplicht wordt niet gerefereerd aan gestandaardiseerde sectorale privacyverklaringen, waardoor de kans reëel is dat het te bereiken resultaat (gestandaardiseerde sectorale privacyverklaringen en het gebruik daarvan) niet wordt bereikt. Derhalve is hiervoor geconcludeerd dat de Europese wetgever er verstandig aan doet om op hoofdlijnen een gestandaardiseerde privacyverklaringen te ontwikkelen, die vervolgens in de lidstaten nader op sectoraal niveau ingevuld kan worden, daarbij rekening houdend met de specifieke kenmerken van de sectoren.

6.3.2 De vorm en inhoud van het zelfreguleringsinstrument privacyverklaring

De zelfregulering ziet op de nadere sectorale invulling van de gestandaardiseerde privacyverklaring. Deze sectorale invulling zal met name betrekking hebben op de inhoud van de privacyverklaring, en niet zozeer op de vorm. De vorm van de gestandaardiseerde privacyverklaring zal op EU-niveau vastgesteld moeten worden, evenals het bredere kader voor de inhoud. Relevant voor de inhoudelijke aspecten die op EU-niveau geadresseerd moeten worden is artikel 14 lid 1 van het voorstel inzake herziening van de Privacyrichtlijn. Daaruit volgt dat de Europese Commissie het aantal te vermelden onderwerpen wil uitbreiden. Het betreft - kort gezegd - de periode dat de persoonsgegevens worden opgeslagen, het recht op toegang, wijziging en verwijdering van de persoonsgegevens, het recht op verzet, het recht om een klacht in te dienen tegen de nationale toezichthouder en de (categorieën) ontvangers van de persoonsgegevens. Indien de verantwoordelijke voornemens is om persoonsgegevens te verstrekken aan derde landen of internationale organisaties dient hij het beschermingsniveau te vermelden dat door die landen of organisaties in acht wordt genomen. Tevens moet in dat geval de verantwoordelijke vermelden of autoriteiten van die landen zich toegang kunnen verschaffen tot de persoonsgegevens.[664] Evenals de artikelen 33 en 34 Wbp, werkt het voorgestelde artikel 14 met open normen.[665] Deze kunnen vervolgens in de gestandaardiseerde privacyverklaring op sectoraal niveau nader worden geconcretiseerd, daarbij rekeninghoudend met het vereiste dat de nadere uitwerking niet in strijd mag zijn met de Privacyrichtlijn en de Wbp.[666]

663 Zie Geelhoed, p. 49.
664 Artikel 14 lid 1 sub c. tot en met g. COM (2012) 11 final.
665 Artikel 14 lid 1 sub h. COM (2012) 11 final.
666 Zie hoofdstuk 3.

Met betrekking tot de nadere uitwerking zou overwogen moeten worden te onderzoeken over welke onderwerpen de betrokkene geïnformeerd wil worden.[667] Voorts is in hoofdstuk 5 geconcludeerd dat een privacyverklaring in principe een werkbaar instrument is om invulling te geven aan de beginselen van transparantie en accountability. Bij het formuleren van de inhoud van de gestandaardiseerde privacyverklaring dienen derhalve de geïdentificeerde aspecten van transparantie in acht te worden genomen, waardoor de privacyverklaring tevens daadwerkelijk betekenis krijgt voor accountability.[668] Daarbij is het van belang dat in de privacyverklaring wordt vermeld welke maatregelen de verantwoordelijke heeft genomen ter controle of de persoonsgegevens worden verwerkt conform het bepaalde in de privacyverklaring.

6.3.3 Binding van belanghebbenden aan zelfregulering

Belangrijk is de vraag naar de grondslag voor binding aan zelfregulering, en welke partijen zoal aan de zelfregulering zijn gebonden. Giesen en Lindahl onderkennen twee grondslagen voor binding aan zelfregulering, te weten de wet en consensus.[669] Met betrekking tot de eerste grondslag bedoelt Giesen dat "…een wet een specifieke grondslag geeft voor de nadere invulling van bijvoorbeeld beroepsregels, waarna dergelijke regels vervolgens vanuit de beroepsgroep zelf (via een overkoepelende organisatie) opgesteld, afgekondigd en eventueel later gewijzigd worden".[670] De binding aan zelfregulering kan ook plaatsvinden doordat de wetgever op enig moment bindende kracht verleent aan een regeling. "Voor vormen van alternatieve regelgeving betekent deze tussenstap via de wetgever dat de beoogde binding aan bepaalde normen in bijvoorbeeld een gedragscode, ook (vooraf of alsnog achteraf) ingebouwd kan worden door een 'wettelijk sausje' daar overheen te gooien, door dus (alsnog) via een wettelijke interventie (extra) gezag en binding mee te geven aan die normen".[671] Met de grondslag consensus doelt Giesen op het eigen gezag van de groepering. Lindahl spreekt niet over consensus, maar over de individuele vrijheid voor zover de autonomie van het individu het grondbeginsel van het privaatrecht is. "Partij kiezen voor zelfregulering is partij kiezen voor horizontale verhoudingen tussen individuen, en dus voor de wederkerigheid waarin de individuele vrijheid gestalte krijgt".[672]

---

667 De resultaten uit het EU Endorse-onderzoek kunnen daarbij mogelijk tentatief zijn.

668 Deze aspecten betreffen (i) de naamgeving, traceerbaarheid en de toegankelijkheid van de privacyverklaring, (ii) de vorm van de privacyverklaring, en (iii) de inhoud, leesbaarheid en begrijpelijkheid van de privacyverklaring.

669 In het navolgende zal blijken dat Giesen nog een derde grondslag onderkent, namelijk open normen uit het BW.

670 Giesen 2007-b, p. 60. Voorbeelden zijn de Advocatenwet, de Gerechtsdeurwaarderswet en de Wet op het notarisambt.

671 Giesen 2007-b, p. 60 e.v. Giesen noemt de Code Tabaksblat als voorbeeld.

672 Lindahl, p. 41.

De vervolgvraag is wie aan de tot stand gebrachte zelfregulering gebonden is. Volgens Lindahl zijn de individuen die de zelfregulering tot stand hebben gebracht, ook degenen die gebonden worden door de zelfregulering. “Naast de binding die aan overheidsregelgeving toekomt vanwege de erkenning van de wet als bron van recht lijkt de binding van zelfregulering uit een eigen bron voort te vloeien, met name uit de vrijheid van individuen om onderling regelingen te treffen, waarbij vrijheid opgevat wordt als identiteit in de zin van ‘co-referentialiteit’: het zijn dezelfde individuen die een rechtsnorm stellen en zich daaraan onderwerpen”.[673]

De groep van belanghebbenden zal met betrekking tot het zelfreguleringsinitiatief primair bestaan uit brancheorganisaties.[674] Het zijn immers deze organisaties die door middel van zelfregulering het gebruik van gestandaardiseerde privacyverklaringen willen reguleren.[675] Schmidt et al. komen in hun onderzoek (2003) tot de conclusie dat Nederland ongeveer 1100 brancheorganisaties kent, en er ten aanzien van de slagkracht veel verschil bestaat tussen brancheorganisaties onderling.[676] Volgens de website www.kennisportal.com zijn er heden ten dage om en nabij 1200 brancheorganisaties. Deze observaties zijn in het kader van het zelfreguleringsinitiatief te kwalificeren als knelpunten. Het is nagenoeg ondoenlijk met 1200 brancheorganisaties tot afspraken te komen. Dit klemt te meer daar er een verschil in slagkracht is geconstateerd tussen brancheorganisaties. Koops et al. stellen: “For self-regulation to work, the stakeholders should be well organized in order to ensure that the people participating in the process know the needs and desires of their colleagues and the people they represent”.[677] Ook Baarsma et al. wijzen op de organisatiegraad van de betrokken belangenorganisaties. “Een sterke verbinding tussen de deelnemers van een bepaalde beroepsgroep of brancheorganisatie zal ertoe leiden dat er een betere sociale controle is en coördinatie mogelijk blijft”.[678] Anderzijds stellen we vast dat de kring van brancheorganisaties in het kader van het zelfreguleringsinitiatief niet zal bestaan uit alle brancheorganisaties, vanwege het feit dat niet alle leden van die brancheorganisaties webdiensten aanbieden. Ten aanzien van de gesignaleerde knelpunten zou daarom moeten worden overwogen waar mogelijk ook koepelorganisaties bij het zelfreguleringsinitiatief te

673 Lindahl, p. 41. Zo ook Geelhoed, p. 49 en Van Driel p. 2.

674 In deze dissertatie kwamen de brancheorganisaties Verbond van Verzekeraars, ANVR, CBW-MITEX, Thuiswinkel.org en NGFG al aan de orde, waarbij in geval van NGFG het wellicht juister is te spreken van een belangenorganisatie.

675 Zo ook Van Driel die benadrukt dat de feitelijke vaststelling van een zelfreguleringsafspraak hoe dan ook door het bedrijfsleven moet geschieden, wil er sprake zijn van zelfregulering. “Anderen – overheid, consumentenorganisaties, andere maatschappelijke groeperingen – kunnen weliswaar aandringen op zelfregulering, al dan niet concrete eisen op tafel leggen en soms als onderhandelingspartner mede vorm geven aan de regels of afspraken, het is het bedrijfsleven dat door middel van zelfregulering haar activiteiten reguleert”. Van Driel, p. 84.

676 Schmidt et al., p. 54.

677 Koops et al., p. 136.

678 Baarsma et al., p. 30.

betrekken. Voorbeelden van dergelijke koepelorganisaties zijn VNO-NCW en MKB-Nederland. Van de 1100 brancheorganisaties zijn 150 aangesloten bij VNO-NCW[679] en 130 brancheorganisaties bij MKB-Nederland.[680] Gezamenlijk vertegenwoordigen zij om en nabij 301.000 ondernemingen. Het onderwerp privacy staat bij beide koepelorganisaties op de agenda. Dit volgt mede uit het bestaan van de Commissie Privacy bij VNO-NCW en de gezamenlijke reactie van beide koepelorganisaties naar de Europese Commissie met betrekking tot herziening van de Privacyrichtlijn.[681] Tevens benadrukken VNO-NCW en MKB-Nederland het belang van zelfregulering. “Self regulation is generally more flexible and can be tailored to changing circumstances and developments. We therefore support the examination of further encouraging self-regulatory initiatives”.[682]

6.3.4 De rechtspositie van de betrokkene

Wat is de betekenis van de voorkeur voor zelfregulering als we deze bezien op de consequenties voor de positie van consumenten of betrokkenen (zoals bedoeld in de Wbp) die niet direct betrokken waren bij de totstandkoming van de zelfregulering? Kunnen zij rechten ontlenen aan de zelfreguleringsafspraak die door de belanghebbenden is overeengekomen? Anders gezegd, kunnen belanghebbenden gebonden worden aan de door hen gemaakte zelfreguleringsafspraak jegens een derde die geen partij is geweest bij de uitwerking van het zelfreguleringsinitiatief? In dit kader is relevant of de zelfreguleringsafspraak valt aan te merken als recht in de zin van artikel 79 RO.[683] Volgens Giesen verkrijgt een regeling die kan worden gekwalificeerd als recht in de zin van artikel 79 RO meer gewicht en status, en daardoor meer invloed.[684] Die invloed uit zich met name in het feit dat de betreffende regeling, vanwege de kwalificatie als recht in de zin van artikel 79 RO, in cassatie toetsbaar wordt. De jurisprudentie laat echter zien dat private regelgeving door de Hoge Raad veelal niet wordt aangemerkt als recht in de zin van artikel 79 RO. Zo overwoog de Hoge Raad in het arrest *Kouwenberg/Rabobank* dat het tussen partijen van toepassingverklaarde Reglement voor de handel op de optiebeurs (RHO) niet voldeed aan de in de rechtspraak van de Hoge Raad ontwikkelde criteria om van recht in de zin van

679 Zie de website van VNO-NCW; www.vnoncw.nl.

680 Zie de website van MKB-Nederland; www.mkb.nl.

681 VNO-NCW en MKB-Nederland reaction on the Communication of the Commission on: “a comprehensive approach on personal data protection in the European Union”, COM (2010) 609/3, d.d. 14 januari 2011. De gezamenlijke reactie is onder meer te vinden op de website www.vnoncw.nl. Ook het kabinet erkent in dezen de ‘statuur’ van VNO-NCW en MKB-Nederland. Kamerstukken II 2009–2010, 31051, nr. 5, p. 31. Daarentegen stelt Berkvens dat sinds de inwerkingtreding van de privacywetgeving de rol van trade associations beperkt is. Berkvens 2009-a, p. 125.

682 VNO-NCW en MKB-Nederland reaction on the Communication of the Commission on: “a comprehensive approach on personal data protection in the European Union”, COM (2010) 609/3, p. 6.

683 Zie voor een meer uitgebreide behandeling onder meer Giesen 2007-b, Asser/Vranken en Lindahl.

684 Giesen 2007-b, p. 46.

artikel 79 RO te kunnen spreken.[685] Ten aanzien van een gedragscode zoals bedoeld in artikel 25 Wbp, concludeert Verkade dat dit geen recht is in de zin van artikel 79 RO. “Vooralsnog houd ik het erop dat zo'n gedragscode louter aan de verklaring van het CBP niet de status van 'recht' in de zin van art. 79 RO ontleent, en ook niet 'formele rechtskracht' jegens diegenen die in de (summiere) voorbereidingsprocedure op de voet van art. 3.4 Awb niet van bezwaren hebben doen blijken. De rechter is mijns inziens niet gebonden aan hetgeen de betrokken branche qua interpretatie van de Wbp in de gedragscode heeft neergelegd, ook niet na de - instemmende - verklaring van het CBP ingevolge art. 25 lid 1 Wbp”.[686] Indien een regeling niet wordt aangemerkt als recht in de zin van artikel 79 RO, betekent dit nog niet dat de betrokkene aan de regeling geen rechten kan ontlenen. Volgens Giesen kan binding aan alternatieve regelgeving tevens voortvloeien uit de open BW-normen, in het bijzonder artikel 3:12 BW en artikel 6:162 BW. Dit is de derde grondslag van binding die Giesen onderscheidt.[687]

> Artikel 3:12 BW
> Bij de vaststelling van wat redelijkheid en billijkheid eisen, moet rekening worden gehouden met algemeen erkende rechtsbeginselen, met de in Nederland levende rechtsovertuigingen en met de maatschappelijke en persoonlijke belangen, die bij het gegeven geval zijn betrokken.
>
> Artikel 6:162 lid 2 BW
> Als onrechtmatige daad worden aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt,…

Illustratief is het *Trombose* arrest, dat duidelijk maakt dat een patiënt rechten kan ontlenen aan een protocol dat is overeengekomen tussen een ziekenhuis en artsen.[688] De Hoge Raad overwoog dat van het ziekenhuis en artsen mag worden verwacht dat zij zich ook richting de patiënt in beginsel houden aan de door henzelf opgestelde voorschriften met betrekking tot verantwoord medisch handelen, en afwijking van die voorschriften slechts aanvaardbaar is indien dat in het belang van een goede patiëntenzorg wenselijk is.[689] Vranken expliciteert het verschil tussen de arresten *Kouwenberg/Rabobank* en *Trombose*. “Ook over het protocol had de Hoge Raad kunnen overwegen dat het geen recht vormde in de zin van art. 79 RO”. En Vranken vervolgt: “Hij heeft de moed gehad om zich los van de criteria van art. 79 RO een oordeel te vormen over het juridisch gehalte van het protocol als

685 HR 11 juli 2003 (*Kouwenberg/Rabobank*), onderdeel 3.5.3.
686 Verkade, nr. 4.13. Zo ook Dommering 2007.
687 Giesen 2007-b, p. 68 e.v. Vergelijk Van Driel, p. 133, 144 e.v.
688 HR 2 maart 2001(*Trombose*), NJ 2001, 649.
689 Onderdeel 3.3.3.

private regelgeving". "Toegespitst op het concrete geval heeft hij de bindende kracht ervan aanvaard en, anders dan met art. 31m RHO, de aansprakelijkheid van de arts gegrond op overtreding van het protocol".[690] Een meer recent voorbeeld met betrekking tot de status van private regelgeving betreft een arrest van de Hoge Raad uit 2011.[691] Huydekoper concludeert dat de Leidraad van de Raad voor de Journalistiek waarop door eiseres een beroep wordt gedaan, niet op één lijn is te stellen met geldend Nederlands recht. "Het gaat hier om een door beroepsgenoten geformuleerd geheel van regels, enigszins vergelijkbaar met de tuchtreglementen en gedragscodes die door verschillende beroepsgroepen zijn ontwikkeld (al-dan-niet op basis van wettelijke bevoegdheden). Voor tuchtrechtelijke regels is in de rechtspraak aangenomen dat overtreding daarvan weliswaar een aanwijzing kan opleveren dat ook een rechtsnorm/zorgvuldigheidsnorm is geschonden, maar niet zonder meer meebrengt dat er van onrechtmatig gedrag sprake is".[692] Bij het *Dexia* arrest concludeert AG Verkade ten aanzien van een gedragscode, zoals bedoeld in artikel 25 Wbp, dat deze gedragscode mogelijk een 'gezichtspunt' of 'essentiële stelling' oplevert indien daar in rechte een beroep op wordt gedaan.[693] Vranken komt tot de meer algehele conclusie dat de mate waarin protocollen, voorschriften en richtlijnen bindend zijn, onder meer afhankelijk is van het antwoord op de vraag hoe en tussen wie deze zijn overeengekomen, waarop ze betrekking hebben, hoe ze zich verhouden tot de 'state of the art', en of de belangen van alle betrokkenen voldoende zijn gewaarborgd.[694]

Wat is, in het licht van het voorgaande, nu concreet de rechtspositie van de betrokkene ten opzichte van een branchelid dat het zelfreguleringsinitiatief onderschrijft? De betrokkene is direct noch indirect partij geweest bij (de totstandkoming van) dit initiatief. Kan de betrokkene daar nu desalniettemin rechten aan ontlenen wanneer een branchelid jegens hem niet handelt conform de inhoud van de privacyverklaring? In paragraaf 6.3.2 zijn de grondslagen van binding aan zelfregulering besproken.[695] Anders dan in de relatie brancheorganisatie en branchelid, ontbreekt de eerder besproken grondslag van consensus tussen een branchelid en de betrokkene ten aanzien van de zelfregulering. Een eventuele binding van het branchelid aan de zelfreguleringsafspraak jegens de consument zou dan moeten voortvloeien uit de open normen van het BW, in het bijzonder artikel 3:12 BW en artikel 6:162 BW.[696] Of de betrokkene rechten kan ontlenen aan de inhoud van de privacyverklaring, is afhankelijk van de omstandigheid of de rechter bij invulling van de open

690 Asser/Vranken, nr. 84.
691 HR 8 april 2011 (*Pretium/Tros*), LJN BP6165.
692 Huydekoper, nr. 22.
693 Verkade, nr. 4.13.
694 Asser/Vranken, nr. 84.
695 De grondslagen betreffen de wet, consensus en de open normen uit het BW.
696 Zoals bleek in paragraaf 6.3.4 is in dit kader relevant het *Trombose* arrest waaruit volgt dat partijen jegens derden gebonden kunnen worden aan afspraken die door henzelf zijn opgesteld.

normen het zelfreguleringsinitiatief in ogenschouw neemt.[697] Dit brengt (rechts)onzekerheid met zich mee. Op grond van de bevindingen uit hoofdstuk 3 kan worden betoogd dat deze onzekerheid grotendeels kan worden weggenomen indien de gestandaardiseerde privacyverklaring kan worden gekwalificeerd als overeenkomst. De gestandaardiseerde privacyverklaring dient in dat geval als aanbod (in de zin van artikel 6:217 lid 1 BW) door het branchelid te worden gepresenteerd indien de betrokkene een dienst of product afneemt via de website van een branchelid, waardoor er een privacyovereenkomst tot stand komt indien de betrokkene het aanbod aanvaardt.[698]

6.3.5 Gebondenheid van branchegenoot die geen lid is van een brancheorganisatie

Een andere relevante vraag is of een branchegenoot die de binnen die branche tot stand gekomen zelfregulering expliciet dan wel impliciet verwerpt, toch gebonden is aan die zelfregulering. In beginsel is deze branchegenoot niet gebonden aan de zelfregulering omdat hij zich niet aan de zelfregulering heeft onderworpen.[699] Verkade wijst in zijn conclusie bij het *Dexia* arrest op de gedragscode die invulling geeft aan de open normen van de Wbp, en stelt vervolgens dat de branchegenoot die de Wbp beperkter interpreteert dan die gedragscode allicht de schijn tegen heeft.[700] Giesen is van mening dat alternatieve regelgeving invloed kan hebben bij rechtsvorming.[701] Hij refereert daarbij aan gedragscodes die een rol kunnen spelen bij de invulling van de open normen uit het BW, in het bijzonder artikel 3:2 BW en artikel 6:162 BW.[702] "Gedragscodes, etc., kunnen daardoor een articulering worden van wat rechtens is".[703] De branchegenoot zou dan gebonden worden aan binnen die branche tot stand gekomen zelfregulering doordat de zelfregulering fungeert als een brugfunctie. "In het schema wetgeving-rechtspraak is de beantwoording van de vraag welke maatschappelijke veranderingen, hoe en in welke mate doorwerken in het burgerlijk recht, voorbehouden aan de wetgeving en de rechtspraak. Zij zijn de sluizen die gepasseerd moeten worden, willen maatschappelijke veranderingen rechtens relevant zijn. Private regelgeving kan hierbij een brugfunctie vervullen tussen wat in bepaalde sectoren van de maatschappij aan kennis, ervaring en inzichten van de direct betrokkenen leeft, en de regel die in die sector moet functioneren. Zij vormt een belangrijke bron van informatie voor de wetgever of de rechter, die veel preciezer is dan verwijzingen naar bijvoorbeeld gebruiken of overtuigingen in de samenleving. In de regel is de informatie ook actueler,

---

697 In de woorden van Vranken: "…of de rechter de moed heeft om zich los van de criteria van artikel 79 RO een oordeel te vormen over het juridische gehalte van de privacyverklaring als private regelgeving". Zie paragraaf 6.3.4.

698 Zie in dit kader paragraaf 3.5.

699 Deze problematiek ligt in lijn met de discussie over 'free riding'. Zie in dat kader Holvast & Gardeniers, p. 50 en Giesen 2007-b, p. 61.

700 Verkade, nr. 4.14.

701 Giesen gaat uitgebreid in op het thema alternatieve regelgeving en rechtsvorming. Giesen 2007-b, p. 91 e.v.

702 Ook artikel 6:248 lid 1 BW kan, zoals blijkt uit paragraaf 3.7.3, in dezen betekenis krijgen.

703 Giesen 2007-b, p. 99.

omdat het bewegingsritme van private regelgeving beter inspeelt op nieuwe ontwikkelingen. In sectoren met een goed georganiseerde private regelgeving kunnen maatschappelijke veranderingen daarom sneller doorwerken in het burgerlijk recht. Voorwaarde is wel dat de wetgever en rechtspraak er open voor staan en, wat de rechtspraak betreft, dat zij de kans krijgt zich uit te spreken".[704] Uit het voorgaande kan worden geconcludeerd dat een branchegenoot die zich niet heeft gecommitteerd aan de tot stand gekomen zelfregulering, dat wil zeggen aan de nadere uitwerking van de informatieplicht op brancheniveau, waarbij de brancheorganisaties zorgdragen voor een nadere sectorale invulling van de gestandaardiseerde privacyverklaringen die op hoofdlijnen door de Europese Commissie is ontwikkeld, onder omstandigheden toch kan worden gebonden aan de zelfreguleringsafspraak.

6.3.6 De positie van de Consumentenbond en de overheid

Voor consumentrelaties zou als nadere waarborg voor het verdisconteren van de belangen van deze betrokkenen (zoals bedoeld in de Wbp), kunnen worden overwogen de Consumentenbond bij het zelfreguleringsinitiatief te betrekken. Als onafhankelijke organisatie zonder binding met enige politieke of levensbeschouwelijke stroming of organisatie, zou de Consumentenbond bij de nadere uitwerking van standaarden voor privacyverklaringen de belangen van consumenten kunnen trachten te behartigen.[705] Dat de Consumentenbond een belangrijke stem kan hebben, blijkt mede uit het feit dat de Consumentenbond is vertegenwoordigd in negen commissies van de Sociaal Economische Raad, alsook dat zij zitting heeft in de Stichting Geschillencommissie voor Consumentenzaken. De vraag is echter welke positie de Consumentenbond in het zelfreguleringsinitiatief zou willen innemen. De keuzemogelijkheid ziet naar mijn mening op een positie waar de Consumentenbond haar stem laat horen ten aanzien van de zelfreguleringsafspraak die op brancheniveau tot stand komt, of op een positie waar de Consumentenbond zich committeert aan de zelfreguleringsafspraak.[706] Mede gezien de door de Consumentenbond gewenste onafhankelijkheid ten opzichte van het bedrijfsleven, lijkt mij het meest voorstelbaar dat zij kiest voor de eerste optie.[707] Bovendien is er nog een aanvullende reden voor betrokkenheid van de Consumentenbond. Hiermee kan het zelfreguleringsinitiatief meer draagvlak en daarmee meer 'waarde' verkrijgen. In de vorige paragraaf is gebleken dat de derde grondslag van binding aan alternatieve regelgeving is

704 Asser/Vranken nr. 91.

705 Consumentenbond Statuten 21 maart 2007, te raadplegen via de website www.consumentenbond.nl.

706 Zo ook Van Driel, p. 85. Vergelijk Berkvens die stelt dat in het verleden consultaties met consumentenorganisaties niet succesvol zijn gebleken. "…and it had been seen that the consultations with consumer organisations had not really been a success". Berkvens 2009-a, p. 128.

707 Volgens Van Driel menen consumentenorganisaties dat overleggen en onderhandelen met het bedrijfsleven over zelfregulering op gespannen voet staat met hun eigenlijke functie als behartiger van consumentenbelangen. Van Driel, p. 89.

gelegen in de open normen uit het BW, in het bijzonder artikel 3:12 BW en artikel 6:162 BW. Des te representatiever het zelfreguleringsinitiatief is, des te waarschijnlijker het wordt dat de rechtsprekende macht dit initiatief in overweging zal nemen bij het invullen van de open normen uit het BW. Daarmee wordt vervolgens de kans vergroot dat een betrokkene rechten kan ontlenen aan de zelfreguleringsafspraak, alsook dat een branchegenoot die zich niet heeft gecommitteerd (of wil committeren) aan de zelfreguleringsafspraak toch gebonden wordt.

Ook de overheid kan een rol spelen bij de totstandkoming van zelfregulering. Van Driel wijst erop dat bij zelfregulering de overheid in drie hoedanigheden kan optreden: als toezichthouder, als onderhandelaar en als subsidiegever.[708] De rol van toezichthouder is wat betreft verwerkingen van persoonsgegevens voorbehouden aan het Cbp. De tweede hoedanigheid is die van onderhandelaar. Het is echter de vraag of het wenselijk is dat de overheid in die hoedanigheid betrokken wordt bij het zelfreguleringsinitiatief.[709] De zelfregulering is immers al wettelijk geconditioneerd. Overigens is het twijfelachtig of de overheid een dergelijke functie ambieert, gezien het feit dat het kabinet ten aanzien van verwerkingen van persoonsgegevens steeds meer verantwoordelijkheden neerlegt bij het bedrijfsleven en burgers.[710] De laatste van de drie, de overheid in de hoedanigheid van subsidieverstrekker, zal de brancheorganisaties mogelijk aanspreken. Dat het zelfreguleringsinitiatief voor hen kosten met zich meebrengt is onontkomelijk. Dit zal door de brancheorganisaties als nadeel worden ervaren, hetgeen mogelijk negatieve effecten heeft op de succesratio van het zelfreguleringsinitiatief. De overheid kan deze ‘hindernis’ deels wegnemen door het beschikbaar stellen van subsidies om daarmee de ontwikkeling van de standaarden in het eerste prille stadium te stimuleren.[711]

6.3.7 Toezicht en handhaving

Uit paragraaf 6.2 volgt dat naleving van zelfregulering en de handhaving daarvan door middel van toezicht, een belangrijke voorwaarde is voor de effectiviteit van zelfregulering. Concreet voor het zelfreguleringsinitiatief omvat toezicht de controle op het daadwerkelijk gebruik door een branchelid van de gestandaardiseerde privacyverklaring, en het conform

---

708 Van Driel, p. 15.

709 Een bijkomend aspect is of in dat geval nog wel kan worden gesproken van zelfregulering. “Zolang het bedrijfsleven de partij is van wie de regels uiteindelijk uitgaan, zal de regeling als zelfregulering aangeduid kunnen worden, zij het dat er dan wel sprake is van opgelegde of afgedwongen zelfregulering”. Van Driel, p. 15.

710 Zie bijvoorbeeld Kamerstukken II 2011-2012, 26 643, nr. 211, p. 7.

711 Het is voorstelbaar dat het kabinet pas tot mogelijke subsidieverstrekking zal overgaan indien het duidelijk is op welke wijze gestandaardiseerde sectorale privacyverklaringen tot stand moeten komen. Het kabinet heeft immers laten weten geen actie te zullen ondernemen ten aanzien van onderwerpen die door de Europese Commissie zijn benoemd in het kader van herziening van de Privacyrichtlijn. Kamerstukken II 2009-2010, 31051, nr, 5, p. 21 e.v.; Kamerstukken II 2010-2011, 32761, nr. 1, p. 15; Zo ook Koops, p. 170.

de standaard handelen.[712] Wanneer zelfregulering aan de orde is, zo benadrukt het kabinet, is het toezicht op de behoorlijke verwerking van persoonsgegevens conform de zelfreguleringsafspraken, niet primair een zaak van de toezichthouder.[713] In geval van zelfregulering legt het kabinet kortom de toezichthoudende taak neer bij de zelfreguleerder. Met betrekking tot het zelfreguleringsinitiatief komt daarmee het toezicht te liggen bij de brancheorganisaties.

De vraag is vervolgens welke mogelijkheden een brancheorganisatie heeft indien een branchelid de privacyverklaring niet gebruikt, dan wel niet handelt conform de inhoud van de privacyverklaring? De grondslag voor binding van het branchelid aan de zelfreguleringsafspraak is gelegen in consensus; dit vanwege de aanvaarding van de lidmaatschapsvoorwaarden. Daarbij is - vanzelfsprekend - van belang dat in die voorwaarden het gebruik van de privacyverklaring en de naleving van de inhoud daarvan verplicht is gesteld. Indien het branchelid zich niet houdt aan de zelfreguleringsafspraak, kan de brancheorganisatie de lidmaatschapsovereenkomst ontbinden. In de regel zullen in de voorwaarden nog andere sancties worden benoemd. Illustratief zijn de lidmaatschapsvoorwaarden van Thuiswinkel.org. Op grond van deze voorwaarden heeft een lid de verplichting een privacyverklaring op zijn website te plaatsen, alsook om die privacyverklaring vooraf inhoudelijk te laten toetsen - en indien nodig in overleg te laten aanpassen - door een juridisch bureau. Uit artikel 5 lid 1 Statuten Thuiswinkel.org valt op te maken dat een lid verplicht is om het bepaalde in de wet, de statuten, het huishoudelijk reglement en andere rechtsgeldig tot stand gekomen besluiten, overeenkomsten en/of reglementen na te leven. Indien een lid zich niet houdt aan zijn verplichting om een privacyverklaring op zijn website te plaatsen, handelt hij in strijd met het bepaalde in artikel 5 lid 1 Statuten Thuiswinkel.org, en kan hij op grond van artikel 5 lid 3 Statuten Thuiswinkel.org worden berispt, beboet, geschorst of worden ontzet uit het lidmaatschap.

6.4 Afronding: aanbevelingen en ambitie

In dit hoofdstuk is onderzocht op welke wijze gestandaardiseerde privacyverklaringen – EU-breed – ontwikkeld kunnen worden. Daarbij is – mede met het begin 2012 verschenen voorstel tot aanpassing van de Privacyrichtlijn op het netvlies - als vertrekpunt genomen dat een gestandaardiseerde privacyverklaring op hoofdlijnen op EU-niveau moet worden ontwikkeld, en dat de sectorale invulling daarvan op nationaal niveau moet plaatsvinden.

712 Dit houdt tevens in dat gecontroleerd dient te worden of het branchelid voldoet aan zijn accountabilityplicht.

713 Kamerstukken II 2009–2010, 31051, nr. 5, p. 29. Vergelijk Teunissen die expliciteert dat volgens de nieuwe reguleringsmodellen het ‘primaire toezicht’ op de naleving van de publiekrechtelijke doelvoorschriften en zorgplichten zoveel mogelijk moeten geschieden door private actoren zelf. Teunissen p.14. Zie ook Kamerstukken II 2005-2006, 27831, nr. 15.

Daarbij is geconcludeerd dat het initiatief voor de ontwikkeling van de gestandaardiseerde privacyverklaring op hoofdlijnen bij de Europese wetgever moet liggen. De sectorale invulling kan vervolgens op nationaal niveau plaatsvinden door sturing via zelfregulering. Vanuit deze keuze voor zelfregulering bij de nadere uitwerking is in het vervolg van het betoog gekeken naar kenmerken en consequenties van sturing via zelfregulering. Tevens is onderzocht welke rol zelfregulering kan vervullen bij een nadere uitwerking van de informatieplicht, via het op brancheniveau ontwikkelen van gestandaardiseerde sectorale privacyverklaringen.

Op grond van het voorgaande kom ik tot de navolgende aanbevelingen:

1. De Europese Commissie dient een gestandaardiseerde privacyverklaring op hoofdlijnen te ontwikkelen;
2. De Europese Commissie dient zelfregulering op nationaal niveau te stimuleren, dat wil zeggen te sturen op een nadere sectorale invulling van de gestandaardiseerde privacyverklaring door brancheorganisaties op nationaal niveau. In Nederland dient deze aanmoediging te worden opgenomen in de Wbp.
3. De vorm van de gestandaardiseerde privacyverklaring dient op EU-niveau te worden ontwikkeld.
4. De inhoud van de gestandaardiseerde privacyverklaring zal zowel op EU-niveau als op nationaal niveau dienen te worden vastgesteld. Concreet zal op EU-niveau de inhoud op hoofdlijnen moeten worden bepaald, die vervolgens op nationaal niveau nader wordt uitgewerkt.
5. Bij het formuleren van de inhoud van de privacyverklaring dienen de geïdentificeerde aspecten van transparantie in acht te worden genomen.[714]
6. In Nederland dient de kring van belanghebbenden te bestaan uit zowel branche- als koepelorganisaties.
7. Indien de betrokkene een dienst of product afneemt via de website van een branchelid, dient door het betreffende branchelid de gestandaardiseerde privacyverklaring als aanbod (in de zin van artikel 6:217 lid 1 BW) te worden gepresenteerd, waardoor er een privacyovereenkomst tot stand komt indien de betrokkene het aanbod aanvaardt.
8. In Nederland dient de Consumentenbond betrokken te worden bij het zelfreguleringsinitiatief.
9. In Nederland dient het kabinet in de hoedanigheid van subsidieverstrekker in de initiële fase betrokken te zijn bij het zelfreguleringsinitiatief.

Als we tenslotte kijken naar het ambitieniveau dat ten aanzien van de gestandaardiseerde sectorale privacyverklaring nagestreefd zou moeten worden, luidt mijn aanbeveling om nader onderzoek te doen naar het gestandaardiseerde modellen die zijn ontwikkeld door

[714] Zie paragraaf 5.3.

Kleimann en Kelly et al. Het doel hiervan is meer inzicht te verkrijgen in de afwegingen en keuzes die zijn en worden gemaakt ten aanzien van deze modellen, en of vervolgens in meer of mindere mate hierbij aansluiting kan worden gezocht. De essentie van het model van Kelly et al. is er in gelegen dat alle wezenlijke informatie met betrekking tot de verwerking van persoonsgegevens in gestandaardiseerde tabelvorm kan worden gepresenteerd op de homepagina van een website.[715] Bekeken vanuit het perspectief van gelaagde privacyverklaringen, zou dit model wellicht als eerste laag kunnen dienen. De tweede laag zou vervolgens kunnen bestaan uit een uitgebreide privacyverklaring, mogelijk geïnspireerd op het model van Kleimann, waarin alle relevante informatie met betrekking tot de verwerking van persoonsgegevens op *abstract* niveau wordt weergegeven. Op de langere termijn zou de verantwoordelijke in de derde laag, naar voorbeeld van de toekomstige inrichting van de website MijnOverheid.nl, op een actieve wijze uitvoering moeten te geven aan het inzage- en correctierecht van de betrokkene.[716] Dat wil zeggen dat de betrokkene op *individueel* niveau, via de derde laag, online inzicht kan verkrijgen in de hem betreffende persoonsgegevens. Op verzoek van de betrokkene dienen onjuiste persoonsgegevens te worden gewijzigd en bovenmatige persoonsgegevens te worden verwijderd.

715 Zie paragraaf 5.4.

716 Kamerstukken II 2011-2012, 26643, nr. 211, p. 15.

Hoofdstuk 7 | Conclusies in kort bestek

7.1 Inleiding

In dit hoofdstuk keren we tenslotte terug naar de drie onderzoeksvragen zoals die in hoofdstuk 1 zijn geformuleerd. Recapitulerend luiden deze onderzoeksvragen als volgt:

1. Wat is de juridische status van een online privacyverklaring?
2. Hoe krijgt de online privacyverklaring in de praktijk vorm en inhoud?
3. In hoeverre, en door welke actor, dient nader op de vorm, inhoud en het gebruik van een online privacyverklaring te worden gestuurd, mede met het oog op ontwikkelingen op EU-niveau?

Aan de hand van de conclusies in de voorgaande hoofdstukken wordt in de navolgende paragrafen voor ieder van deze vragen kort de centrale bevindingen samengevat.

7.2 Conclusie ten aanzien van de juridische status van een online privacyverklaring

In hoofdstuk 2 is de privacyverklaring geanalyseerd vanuit het perspectief van de Wbp. Uit deze analyse volgt dat de verantwoordelijke op grond van de artikelen 33 en 34 Wbp een redelijk open geformuleerde informatieplicht heeft die hij jegens de betrokkene in acht dient te nemen. Aan de hand van de gehanteerde open normen zal de verantwoordelijke een nadere invulling moeten geven waar het de elementen betreft waarover een betrokkene geïnformeerd dient te worden. In hoofdstuk 2 is vervolgens geconcludeerd dat een privacyverklaring een instrument is met behulp waarvan de verantwoordelijke kan voldoen aan zijn informatieplicht zoals die volgt uit de artikelen 33 en 34 Wbp. Met behulp van deze privacyverklaring kan de verantwoordelijke de inhoud, en daarmee de uitwerking, van de informatieplicht concretiseren.

In hoofdstuk 3 is de privacyverklaring geanalyseerd vanuit een privaatrechtelijk perspectief. Daarbij is onderzocht in hoeverre deze verklaring aangemerkt kan worden als een privaatrechtelijke relatie, namelijk als privacyovereenkomst. Geconcludeerd is, dat de verantwoordelijke en de betrokkene via een privacyovereenkomst de informatieplicht nader kunnen invullen. De inhoud van de privacyovereenkomst wordt echter begrensd door de Wbp. Dit betekent dat de afspraken die de verantwoordelijke en de betrokkene in de privacyovereenkomst vastleggen niet in strijd mogen zijn met de Wbp. Hiernaast wordt de invulling en handhaving van de privacyovereenkomst nader ingekaderd door de bepalingen uit het Burgerlijk Wetboek, waaronder niet alleen de algemene regelingen maar ook de

specifieke bepalingen inzake elektronisch contracteren die hun oorsprong vinden in Europese richtlijnen.

Concluderend kan wat betreft de juridische status van de privacyverklaring worden vastgesteld dat niet alleen de Wbp hiertoe relevante bepalingen bevat, maar dergelijke bepalingen al naar gelang de context ook kunnen voortvloeien uit het Burgerlijk Wetboek.

7.3 Conclusie ten aanzien van vorm en inhoud van de online privacyverklaring in de praktijk

Behalve naar de status van de privacyverklaring, is in hoofdstuk 2 ook in theoretische zin gekeken naar de wenselijke vorm en inhoud van de online privacyverklaring. Het is op deze aspecten dat de regelgever, meer specifiek de Groep Gegevensbescherming Artikel 29, in een nadere uitwerking heeft voorzien. Deze is van mening dat de informatie aan de betrokkene rechtstreeks op het scherm dient te worden gepresenteerd, zonder dat de betrokkene zelf actie hoeft te ondernemen om toegang te krijgen tot de via de privacyverklaring aangeboden informatie. De Groep Gegevensbescherming Artikel 29 geeft daarom de voorkeur aan het presenteren van de informatie aan de hand van tekstvensters op het moment dat de persoonsgegevens worden verzameld. Tevens opteert de Groep voor een getrapte verstrekking van informatie. De vervolganalyse in hoofdstuk 2 liet overigens zien dat ondanks deze nadere concretisering door de Groep in de literatuur discussie blijft bestaan over de noodzakelijke elementen van de privacyverklaring. Vanuit deze constatering is in hoofdstuk 4 de stap gezet om in empirische zin te kijken naar de invulling van de privacyverklaring. Dat is gedaan via een onderzoek onder 257 online winkels in de marktsegmenten Verzekeringen, Reizen en Kleding.

Uit dit onderzoek volgt dat in 76% van de gevallen de verantwoordelijke een privacyverklaring op zijn website heeft geplaatst. Tevens wordt duidelijk dat wat betreft de vorm van de privacyverklaring, 92% van de verantwoordelijken de privacyverklaring aanbiedt via een hyperlink. Uit de theoretische analyse bleek dat het aanbieden van een privacyverklaring via een hyperlink juist niet de voorkeur geniet van de Groep Gegevensbescherming Artikel 29. Ook blijkt uit het empirisch onderzoek dat in 99% van de gevallen de privacyverklaring niet in de door de Groep Gegevensbescherming Artikel 29 voorgestelde getrapte vorm wordt aangeboden. Bovendien blijkt de button van de privacyverklaring bij vrijwel geen van de onderzochte websites in een oogopslag zichtbaar. In 92% van alle gevallen dient de betrokkene te scrollen voordat de ‘hyperlinkbutton’ van de privacyverklaring op de homepagina zichtbaar wordt. Bovendien plaatst 72% van de verantwoordelijken de button van de privacyverklaring onderaan de homepagina. Concluderend kan worden gesteld dat de resultaten uit het empirisch onderzoek op veel

onderdelen een nogal afwijkend beeld vertonen ten opzichte van hetgeen in de theoretische analyse is vastgesteld. In ieder geval kan worden geconcludeerd dat de praktijk het advies van de Groep Gegevensbescherming Artikel 29 breed niet opvolgt.

Het empirisch onderzoek laat verder zien dat er wat betreft de inhoud van de privacyverklaringen een grote variëteit aan verklaringen bestaat. Zo worden zeer uitgebreide privacyverklaringen gehanteerd, maar ook privacyverklaringen die slechts enkele regels omvatten. Met betrekking tot de identiteit van de verantwoordelijke maakt 4,1% van de verantwoordelijken daarvan geen melding in de privacyverklaring, terwijl in 63% van alle gevallen de handelsnaam van de verantwoordelijke kenbaar wordt gemaakt. Tegelijkertijd voldoet van alle privacyverklaringen 90% aan de verplichting tot het kenbaar maken van het doel van verwerking. In hoofdstuk 2 is gerefereerd aan de 'passieve' informatieplicht zoals die volgt uit artikel 35 Wbp en artikel 41 Wbp. Op grond van artikel 35 lid 1 Wbp heeft de betrokkene het recht om zich te wenden tot de verantwoordelijke met het verzoek hem mede te delen of persoonsgegevens van hem worden verwerkt. De verantwoordelijke heeft op grond van hetzelfde lid de plicht om de betrokkene binnen vier weken schriftelijk te informeren of hem betreffende persoonsgegevens worden verwerkt. Uit het empirisch onderzoek volgt dat in 44% van alle gevallen geen melding wordt gemaakt van het recht van de betrokkene op toegang tot zijn persoonsgegevens. Ook heeft de verantwoordelijke op grond van artikel 41 lid 3 Wbp de plicht om de betrokkene te informeren dat hij zich kan verzetten tegen het voornemen van de verantwoordelijke om persoonsgegevens aan derden te verstrekken of voor rekening van derden te gebruiken met het oog op werving voor commerciële of charitatieve doelen. Uit het empirisch onderzoek blijkt dat 24% van de verantwoordelijken geen melding maakt van het recht van de betrokkene om zich, afhankelijk van de situatie, te verzetten tegen de verwerking van zijn persoonsgegevens. Tevens laat het empirisch onderzoek zien dat de elementen zoals genoemd in tabel 2.5 veelal niet of niet volledig in de privacyverklaring worden opgenomen.

Geconcludeerd kan dan ook worden dat de dagelijkse praktijk wat betreft het hanteren van privacyverklaringen, alsmede de vorm en inhoud daarvan, een in diverse opzichten afwijkend beeld ten opzichte van de theoretische observaties laat zien. Met het oog op het voornemen van de Europese Commissie om eventueel te sturen op het ontwikkelen en gebruik van gestandaardiseerde privacyverklaringen, is het van belang dat het empirisch onderzoek lijkt aan te tonen dat sturing vanuit brancheniveau ten aanzien van het gebruik van privacyverklaringen effect sorteert.

7.4 Conclusie ten aanzien van het nader sturen op vorm, inhoud en het gebruik van een online privacyverklaring, mede met het oog op ontwikkelingen op EU-niveau.

De hoofdstukken 2 en 5 maken duidelijk dat meerdere instanties wijzen op het belang van transparantie en accountability in relatie tot de verwerking van persoonsgegevens. Zo maakt de Europese Commissie in de plannen voor de herziening van de Privacyrichtlijn duidelijk meer dan in het verleden belang toe te kennen aan het transparantie- en accountability beginsel. De privacyverklaring lijkt als zodanig een zeer werkbaar instrument om invulling te geven aan beide beginselen. Het empirisch onderzoek toont echter aan dat de praktijk veelal een ander beeld laat zien. In ieder geval bieden de onderzochte privacyverklaringen niet de beoogde transparantie. Bovendien blijkt niet alleen niet te worden voldaan aan het gepropageerde belang van transparantie. Ook wordt niet voldaan aan de maatstaf zoals die zal worden gesteld via, de door de Europese Commissie geambieerde invulling van, het beginsel van accountability.
Wil de privacyverklaring daadwerkelijk als instrument van betekenis kunnen zijn voor transparantie en accountability, dan laat het onderhavige onderzoek zien dat met de volgende aspecten in ieder geval rekening gehouden zal moeten worden:

1. De naamgeving, traceerbaarheid en de toegankelijkheid van de privacyverklaring;
2. De vorm van de privacyverklaring;
3. De inhoud, leesbaarheid en begrijpelijkheid van de privacyverklaring.

Van belang is verder dat onderzoek in de Verenigde Staten naar het gebruik van privacyverklaringen de hypothese lijkt te ondersteunen dat de gewenste transparantie mogelijk effectiever kan worden gerealiseerd via het ontwikkelen van gestandaardiseerde privacyverklaringen. Ook het empirisch onderzoek lijkt erop te duiden dat sturing op brancheniveau ten aanzien van het gebruik van privacyverklaringen effect sorteert. Het onderzoek in de Verenigde Staten lijkt bovendien aan te tonen dat sturing door de wetgever op het gebruik van privacyverklaringen effect sorteert op de ontwikkeling van privacyverklaringen. De Europese Commissie, tenslotte, overweegt te gaan sturen op het ontwikkelen en gebruik van gestandaardiseerde privacyverklaringen. Kortom, sturing op het ontwikkelen en gebruik van gestandaardiseerde privacyverklaringen is, redenerend vanuit transparantie en accountability, een ontwikkeling waar bij de toekomstige ontwikkeling van transparantie inzake de verwerking van persoonsgegevens zeker rekening mee gehouden dient te worden.

Vanuit deze constatering is vervolgens in hoofdstuk 6 onderzocht op welke wijze gestandaardiseerde privacyverklaringen – EU-breed – ontwikkeld zouden kunnen worden. Daarbij is – mede met het begin 2012 verschenen voorstel tot aanpassing van de Privacyrichtlijn op het netvlies - als vertrekpunt genomen dat een gestandaardiseerde privacyverklaring op hoofdlijnen op EU-niveau moet worden ontwikkeld, en dat de sectorale

invulling daarvan op nationaal niveau moet plaatsvinden. Specifiek ten aanzien van het initiatief voor de ontwikkeling van op hoofdlijnen gestandaardiseerde privacyverklaringen zal, zo is de conclusie van dit onderzoek, het initiatief bij de Europese wetgever moeten liggen. De sectorale invulling dient vervolgens op nationaal niveau plaats te vinden door sturing via zelfregulering. Tenslotte zouden brancheorganisaties kunnen sturen op een verplicht gebruik door haar leden van de gestandaardiseerde sectorale privacyverklaringen.

Summary

Chapter 1

In the Netherlands, the rules regarding processing personal data are in particular laid down in the Personal Data Protection Act (*Wet bescherming persoonsgegevens* – Wbp). The Wbp came into force in 2001 and implements the European Privacy Directive of 1995. An important provision in both the Directive and therefore also the Wbp concerns transparency in relation to data processing. The Wbp therefore contains an obligation to provide information in accordance with Articles 33 and 34 Wbp, which the data controller is required to take into account when personal data are processed. As stated, the abovementioned articles are a development of the transparency principle – which is not explicit as such in the Wbp – and certainly also of the 'fair processing' principle laid down in Article 6 Wbp.
In everyday practice it turns out that an online privacy statement is a popular instrument for the data controller to attempt to comply with the obligation to provide information based on the Wbp via his website. The use of this tool raises various legal questions, however, questions that concern both the Wbp and the private law context in which agreements on the processing of personal data take shape. Starting from this finding, the following research questions are central:

1. What is the legal status of an online privacy statement?
2. How does an online privacy statement acquire its form and content in practice?
3. To what extent, and through which party, is it necessary to adjust the form, content and use of an online privacy statement, partly with a view to developments at EU level?

Chapter 2

Chapter 2 includes first of all a more detailed exploration of the obligation to provide information as set out in the Wbp, in order then to define the privacy statement as a legal instrument.
On the grounds of Article 33 and 34 Wbp, the data controller has to inform the data subject if his or her personal data are being processed. Thus the data controller is required to make his identity known as well as the purposes of the processing for which the data are intended. For the rest, the data controller is required to provide the data subject with the information that is required based on the nature of the data and/or the circumstances under which the data are obtained and/or the use that is made of the data. It also transpires from this exploration that more detailed rules for cookies are also relevant to the theme of this dissertation. The rules in relation to applying and reading cookies are set out in the Universal Service and End Users Decree (*Besluit universele dienstverlening en*

eindgebruikersbelangen – BUDE), but will eventually be implemented in the Telecommunications Act (*Telecommunicatiewet*). The expectation is that the Wbp will, in addition, be declared to apply in full to the use of cookies. The consequence is that the data controller will have to take into account Articles 33 and 34 Wbp as well as the specific rules in the Telecommunications Act when using cookies.

The data controller has to inform the data subject in order to label the data processing as lawful, but also because the data controller has a duty of care towards the data subject. The obligation to provide information is in any case a development of the 'fair processing' principle set out in Article 6 Wbp, as well as of the transparency principle. While it is true that this transparency principle is mentioned in the considerations in Privacy Directive 95/46/EC, it is not expressly included in the system of provisions, nor is it in the Wbp.

The Safety and Personal Privacy advisory body (Brouwer-Korf Commission), the Dutch Data Protection Authority (DPA) and the Scientific Council for Government Policy (WRR) emphasise the need for transparency. The data subject has to know why, where and which data are collected about him and used and by whom. The Brouwer-Korf Commission concluded that, given the developments in the technology, the obligation to provide information in the Wbp can no longer provide adequate safeguards, the consequence being that we only have an idea about what has to happen with data in the first instance but not what subsequent organisations do with those data. At a European level, the Article 29 Data Protection Working Party, the EDPS and the European Commission have made statements about transparency. The EDPS is of the view, among other things, that Articles 10 and 11 in the Privacy Directive need to be strengthened in such a way that the data collector is obliged to provide the information in a clear, obvious and comprehensible manner. The European Commission and the Article 29 Data Protection Working Party have made it clear that the current provisions regarding the information to be provided to the data subject are not adequate. The European Commission is therefore considering including a general principle of transparent processing of personal data in the revised privacy directive. The Dutch cabinet has also looked several times at the importance of transparency, but does not see any reason to revise the general wording of Articles 33 and 34 Wbp. According to the cabinet this also applies to the rights of access, rectification and objection. The cabinet does, however, intend to oblige the data collector to announce the storage time limits that have been decided and to clarify what will happen to the personal data that have been processed at the end of that time. The cabinet is also considering introducing a separate scheme with specific transparency obligations for profiling purposes, including explaining the purpose of the processing and the categories used in this regard.

It has been noted several times in the Dutch literature that the data controller uses a privacy statement to comply with his obligation to provide information pursuant to Articles 33 and 34 Wbp. The privacy statement can also play a role here when complying with the obligations to provide information that apply to the use of cookies. It is relevant here that the Article 29

Data Protection Working Party is of the view that crucial information about the use of cookies must not be hidden away in a privacy statement. This means that merely using a privacy statement is not sufficient when informing the data subject about the use of cookies.

The Article 29 Data Protection Working Party has drawn up a list of the elements that have to appear as a minimum in a privacy statement. There are a number of arguments in favour of further development of the open standards in Article 33 and 34 Wbp as proposed by the Article 29 Data Protection Working Party. In the first place it would be possible to take the view on the basis of the transparency principle that the information the data controller has to provide has to be as extensive as possible and therefore, as regards the content of a privacy statement, it is not sufficient to be satisfied with simply repeating a number of legal provisions from the Wbp or simply stating that the personal data will be processed in accordance with the Wbp. The foregoing is all the more important now that the Explanatory Memorandum to the Wbp has pointed out that the threat to personal privacy in the information society consists precisely of the numerous possibilities for processing personal data without the knowledge of the data subject. The threat identified in the Explanatory Memorandum can be addressed by including as much relevant information as possible about the processing of personal data in a privacy statement. Zwenne et al. argue in this context that the data subject's position in relation to the data controller depends on what the data subject knows about the data which the data controller is processing about him. Second, a list of elements that have to be included creates more clarity for the data controller. In this case he does not, as it were, need to 'rack his brains' about which elements he needs to include and elaborate on in his privacy statement in order to ensure proper and careful processing as regards the data subject. Third, this also creates a more transparent situation for the data subject, so he has more insight into the processing operations, so he knows which personal data the data controller is processing, as well as the manner in which the data controller is or is not protecting and guaranteeing his personal privacy.
The Working Party has also stated that it prefers multi-layered privacy statements. The recommendations of the Article 29 Data Protection Working Party are in any case not binding, which is a relevant point, given that the list contains many elements where it is unclear whether it is compulsory to provide these on the basis of Articles 33 and 34 Wbp. In the Guidelines on the Publication of Personal Data on the Internet, the DPA conforms to the recommendations of the Article 29 Data Protection Working Party and gives an example of privacy statements. These Guidelines are formally not legally binding on the data controller either. Stated briefly, it is up to the data controller himself to decide whether he wishes to put a privacy statement on his website, and also to make his own choices about the form and content of the privacy statement. If the data controller is a member of a special interest group it may happen that he is subject to certain obligations on the basis of his membership as regards the use of privacy statements.

On the basis of the literature review conducted in chapter 2, one can first conclude that the calls for transparency in relation to processing personal data are becoming more and more urgent. Second, it can be concluded that, reasoning from the importance of transparency, the current provisions in the Privacy Directive and the Wbp regarding the information to be provided to the data subject are inadequate. It is therefore expected that the transparency principle will be clarified in the revised Privacy Directive. Lastly, it can be concluded that a privacy statement is an instrument which can be used by the data controller to comply with his obligation to provide information, and the content of which makes the effects of this obligation more concrete.

Chapter 3

Chapter 3 concentrates on privacy statements as seen from the perspective of the Dutch Civil Code, and in particular the law on contracts. It can be concluded that the data controller is making an offer to the data subject by means of a privacy statement regarding the manner in which he intends to process personal data. Should the data subject accept the data controller's offer then the result is a privacy agreement. The content of the privacy agreement is bound by the Wbp. This means that the agreements which the data controller and the data subject lay down in the privacy agreement must not be in conflict with the Wbp. The privacy agreement can be used as a tool to implement the information obligation deriving from Articles 33 and 34 Wbp. The data controller may in that case take on obligations that go beyond the obligations arising for him from the Wbp. The data controller and the data subject are, however, free to include arrangements in the privacy agreement that do not necessarily have to be included on the grounds of the Wbp.

There are a number of advantages and disadvantages as regards using an agreement as a tool to formalise the obligation to provide information (Articles 33 and 34 Wbp). Starting with the advantages, one can first point to the possibility of making the open standards from Articles 33 and 34 Wbp more concrete. On the basis of a privacy agreement, the data controller and the data subject make it concretely clear under which circumstances they are of the view that sufficient information has been provided so that proper and careful processing of personal data can take place. The consequence of this concretisation is to strengthen the data subject's legal position, given that the privacy agreement makes it clear what the data controller will do or omit to do. A second advantage may be found in raising the awareness of the data controller and the data subject as regards processing personal data. In other words, concluding an 'agreement' contributes to awareness-raising. It is after all not inconceivable that the data controller, when drawing up and entering a privacy agreement, will be more aware that he has obligations towards the data subject as regards processing personal data as well as which concrete obligations he is taking on himself. The

data subject will also be more aware that his personal data are being processed, and which data these are.

But there are also disadvantages attached to the use of a privacy agreement. First, uncertainty remains about the question whether the agreed content complies sufficiently with the requirements of Articles 33 and 34 Wbp. Moreover, the data subject will have no influence in actual practice, and will therefore not be involved in drawing up the privacy agreement. It is also expected that the data subject will not be put in a position to change the content of the privacy agreement. It is moreover not entirely inconceivable that the data subject, if he rejects the content of the privacy agreement, will not be given any chance at all to buy a product via the website. In addition, how does the data subject know whether the privacy agreement is being infringed or not? And even if the data subject has access to a number of legal recourses on the basis of the Civil Code, it will still be difficult for him to have a clear view of these legal recourses and how to apply these. The data controller may also have objections to the use of a privacy agreement. There is after all continuing uncertainty whether acceptance of the privacy agreement by the data subject is actually legally valid. The data subject can state that he has read and understood the privacy agreement, but is this really the case? The data controller himself takes on obligations on the grounds of the privacy agreement. However, the more obligations he takes on himself, the greater the chance that he will fall short vis-à-vis the data subject. Or there is a good chance that the data controller will restrict the amount of information provided in the privacy agreement as far as possible and take on as few obligations as possible.

In the light of the foregoing, the conclusion is that a privacy agreement can be used as a instrument to formalise the obligation to provide information on the basis of Articles 33 and 34 Wbp. But this still only applies at the ‘individual’ level. This means that only the data controller and the data subject are involved as parties in creating and implementing the privacy agreement, which may give rise to legal inequality and legal uncertainty.

Chapter 4

Chapter 4 gives an account of an investigation into 257 online shops in the Insurance, Travel and Clothing industries. The content of the privacy statements provided by the online shops involved in the research has been tested against items that do not per se need to be provided on the grounds of the Wbp. The purpose of the empirical research is to clarify the manner in which the obligation to provide information is given shape and content in day-to-day practice; this has not only been tested against the minimum level stipulated by the Wbp. It is important in this regard to emphasise that the data controller, on the basis of Articles 33 and 34 Wbp, does not have to mention a subject in a privacy statement if this is not relevant

in the context of the obligation to provide information. The fact that a certain subject is not included in a privacy statement therefore does not mean anything as such. The research was also intended to provide an insight into the degree to which the elements in the list of minimum information that has to be provided drawn up by the Article 29 Data Protection Working Party is applied by data controllers. The relevant results have been extrapolated from the specific industry stated below. It should be noted here that in 24% of the cases examined, the website did not include any privacy statement. The results presented below therefore concern the cases (n=196; 76%) where a privacy statement was available.

Form and recognisability of the privacy statement

- In 92% of cases the privacy statement was provided by means of a hyperlink.
- In 99% of cases the privacy statement was not presented in a multi-layered form.
- In 44% of cases 'privacy' was used to refer to the button for the hyperlink or pop-up screen, and 19% of sites used the term 'privacy statement'.
- In 24% of cases the button for the hyperlink was not located on the home page.
- In 72% of cases the button for the hyperlink was at the bottom of the home page.
- In 92% of cases the data subject needed to scroll down before the button for the hyperlink appears on the home page.
- In 91% of cases the data subject was not given the opportunity to save the privacy statement.

Content: obligatory elements – identity of the data controller and purpose of the processing on the grounds of Article 33 and 34 Wbp

- In 4.1% of cases the privacy statement made no mention of the data controller's identity.
- In 63% of cases the trading name was mentioned in the privacy statement. In none of the cases was the name of the natural person stated if the online shop was run under sole proprietorship. The statutory name was missing in 33% of cases.
- In 90% of cases the purpose of the processing was stated.

Content: right of access, rectification, removal and objection (passive information obligation):

- 44% of the sites made no mention of the right of data subjects to access their personal data.
- In 48% of cases no mention was made of the right of the data subject to have his personal data rectified.
- In 74% of cases no mention was made of the right of the data subject to have his personal data removed.
- In 24% of cases no mention was made of the right of the data subject to object to the processing of personal data, regardless of the situation.

Content: the purpose of the privacy statement

- In no instance did the privacy statement state that the data controller wished to comply with its obligation to provide information on the grounds of the Wbp by means of the privacy statement.

Content: data controller's physical and electronic address

- In 79% of cases the data controller's physical address was not mentioned.
- In 54% of cases the data controller's electronic address was not mentioned.

Content: processing special categories of data

- In 80% of cases it was not stated or explained that special categories of data were being processed.

Content: obligatory or optional provision of information

- In 96% of cases it was not stated whether providing certain information was obligatory or optional.

Content: categories of recipients

- In 84% of cases it was not stated for which (categories of) recipients within the data controller's organisation the collected personal data were intended.

Content: storage time limits

- In 93% of cases the length of the storage time limit for collected personal data was not stated.

Content: use of cookies

- In 30% of cases no mention was made of whether the website did or did not make use of cookies.

Content: security measures

- In 46% of cases it was not stated whether security measures had been put in place in order to guarantee, for example, the authenticity, integrity and confidentiality of personal data.

Content: notification to the Dutch Data Protection Authority

- In 64% of cases the website did not state that a processing operation had been notified to the Dutch Data Protection Authority.

Content: data controller's contact person

- In 61% of cases no mention was made of the name and address of the person the data subject had to approach to exercise his rights.
- In 63% of cases the name of the department or officer who was responsible for answering questions concerning personal data processing was not mentioned.

Content: provision of personal data to third parties

- In 20% of cases it was not stated whether personal data would or would not be provided to third parties.
- In 52% of cases no third parties were mentioned.
- In 96% of cases it was not stated whether personal data might or might not be provided to third parties in other countries.
- In 85% of cases it was not stated whether third parties would guarantee the confidentiality and/or protection of personal data.

Content: legal measures

- In 87% of cases no mention was made of the legal measures the data subject could take if the data controller acted incorrectly when processing personal data or acted unlawfully towards the data subject.

Content: amendment to the privacy statement

- In 48% of cases the data controller reserved the right to modify the content of the privacy statement unilaterally.
- In the instances where the data controller reserved the right to modify the privacy statement unilaterally, in 71% of cases the data subject himself had to regularly consult the privacy statement on the website in order to see whether there had been changes or not.

Privacy statement and electronic general terms and conditions

- If the data controller had a privacy statement, as well as electronic general terms and conditions, then in 24% of cases there were also material provisions included in those electronic general terms and conditions concerning processing of personal data.

Online insurers, travel agents and clothing shops may be members of an industry organisation. These special interest groups may require obligatory use of a privacy statement. To these three industries, the special interest group Thuiswinkel.org is relevant, given that this special interest group makes it compulsory to use a privacy statement. Last but not least, the Dutch Association of Insurers is relevant to online insurers. The use of a privacy statement is also compulsory on the grounds of membership of that organisation. It follows from the empirical research that, as regards the use of a privacy statement, it makes

a difference within the Insurance industry whether the online insurer is a member of a special interest group. In this respect, membership of the Dutch Association of Insurers is more significant than membership of Thuiswinkel.org. One can also infer from the empirical research that it is relevant whether an online travel agent or clothing shop is a member of Thuiswinkel.org: there are a lot of statistically significant differences in this regard. Thus the analyses make it clear that obligatory use of a privacy statement, which is imposed by the special interest groups Dutch Association of Insurers and Thuiswinkel.org, has an effect.

Chapter 5

The importance of both transparency and accountability is pointed out on several occasions. A privacy statement appears in principle to be a workable tool to realise both these principles. Research (particularly in the United States) has shown, however, that if a privacy statement is actually going to mean something as regards transparency and accountability, it is necessary to take account of the following aspects:

1. The title, traceability and accessibility of the privacy statement;
2. The form of the privacy statement;
3. The content, readability and comprehensibility of the privacy statement.

The empirical research presented in chapter 4 shows that the use of privacy statements is not unambiguous. If the results of the research are compared with the above transparency aspects, one can conclude that the privacy statements that were researched do not offer the intended transparency. Previous empirical research carried out into the use of privacy statements in the Netherlands seems to confirm this picture. This also has the consequence that privacy statements as these are currently usually applied in practice do not comply with the yardstick that can be set on the basis of the principle of accountability. Accountability could after all mean that the information has to be transparent in accordance with the above-mentioned three aspects.

When the transparency aspects that have been identified are compared with research into privacy statements that was carried out in the United States, we can see that these aspects are not or hardly applied. It is not however possible to draw any unambiguous conclusions about the precise reason for this. One possible explanation is that in the United States, there is no pressure or hardly any pressure from the authorities or private sector to use privacy statements. The absence of transparent privacy statements has led to the hypothesis in the United States that the required degree of transparency could be achieved by developing standardised privacy statements.

The European Commission is also considering emphasising the development of standardised privacy statements. The Commission has however said nothing about the manner in which this could be achieved in practice, except that: “The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary”. The question then is what responsibility the European Commission and/or Dutch legislators will need to accept with regard to the development of standardised privacy statements. The observation that the empirical research in this dissertation demonstrates that pressure as regards the use of privacy statements at industry level appears to have an effect is also relevant in this context. Starting from this observation, we can ask whether industry organisations should not be given a role in the development of standardised privacy statements. Chapter 6 therefore looks at what role self-regulation can play as regards the development and use of standardised privacy statements, and what the legal status of such self-regulation would be.

Chapter 6

Chapter 6 looks at how standardised privacy statements could be developed throughout the entire EU. The point of departure here – also with a view to the proposal to amend the Privacy Directive, which appeared at the start of 2012 – is that the main aspects of a standardised privacy statement should be developed at EU level, and that the industry-based implementation should take place at national level. Here we conclude that the initiative to develop a standardised privacy statement is generally the obligation of the European legislators. The industry-wide implementation can then take place at national level by means of self-regulatory pressure. Starting from this option of self-regulation as regards the detailed implementation, the argument continues by looking at the features and consequences of pressure through self-regulation. We also look at the role that self-regulation can play in the further detailed implementation of the obligation to provide information by developing standardised industry-wide privacy statements.

On the basis of the various findings, chapter 6 then makes the following recommendations:

1. The European Commission should develop a general standardised privacy statement;
2. The European Commission should encourage self-regulation at national level, which means pushing for more detailed industry-wide implementation of the standardised privacy statement by industry organisations at national level. This stimulus needs to be included in the Wbp in the Netherlands.
3. As regards the form of the standardised privacy statement, the necessary first move has to be made at EU level.

4. The content of the standardised privacy statement will need to be decided at both EU and national level. In concrete terms, the main aspects will need to be decided at EU level, after which this can be developed further at national level.
5. It is necessary to take into consideration the transparency aspects that have been identified when formulating the content of the privacy statement.
6. The circle of interested parties in the Netherlands needs to consist of industry as well as umbrella organisations.
7. If the data subject purchases a service or product through the website of an industry member, the industry member in question needs to present the standardised privacy statement as an offer (in the meaning of Article 6.217 para.1 Dutch Civil Code[717]), so a privacy agreement is created if the data subject accepts the offer.
8. In the Netherlands the Consumers' Association needs to be involved, or needs to take on a role in the self-regulation initiative.
9. In the Netherlands the cabinet needs to be involved as a subsidy provider during the initial phase of the self-regulation initiative.

If we look at the level of ambition that should be aimed at as regards the standardised industry privacy statement, the recommendation is to carry out further research into the standardised models that have been developed by Kleimann and Kelly et al. The purpose of this is to gain more insights into the considerations and choices that have been and are being invoked with regard to these models, and whether it is possible to link up with these to a lesser or greater extent. Kelly et al.'s model basically states that all essential information in relation to the processing of personal data can be presented in a standardised table form on the home page of the website. Seen from the perspective of layered privacy statements, this model could well serve as the first layer. The second layer could then consist of a detailed privacy statement, possible inspired by the Kleimann model, where all the relevant information in relation to the processing of personal data is presented at an *abstract* level. In the long run the data controller would have to implement the data subject's right of access and correction in an active manner in the third layer, according to the example of the future organisation of the MijnOverheid.nl website. This means that the data subject could gain an online insight into the personal data that concern him, at an *individual* level, in the third layer. Incorrect personal data would have to be corrected and excessive personal data removed at the data subject's request.

[717] Burgerlijk Wetboek

Chapter 7

Chapter 7 returns to the three research questions as formulated in chapter 1. These research questions are recapitulated below:

1. What is the legal status of an online privacy statement?
2. How does an online privacy statement acquire its form and content in practice?
3. To what extent, and through which party, is it necessary to focus on the form, content and use of an online privacy statement, partly with regard to developments at EU level?

We can conclude the following as regards the legal status of the privacy statement:

1. A privacy statement is an instrument which the data controller can use to comply with his obligation to provide information pursuant to Articles 33 and 34 Wbp. The data controller can formalise the content and therefore the implementation of the obligation to provide information by means of this privacy statement;
2. The data controller takes obligations on himself on the basis of the privacy agreement. The content of the privacy agreement is, however, limited by the Wbp. This means that the agreements which the data controller and the data subject lay down in the privacy agreement must not conflict with the Wbp. In addition the substance and enforcement of the privacy agreement also have to be seen in the context of the provisions of the Dutch Civil Code, including not only the general rules but also specific provisions regarding electronic contracts that originate in European directives.
3. Not only does the Wbp contain relevant provisions in this regard, but such provisions can also be derived from the Civil Code, depending on the context.

In connection with the manner in which the online privacy statement takes it practical form and content, we can conclude that as regards making use of privacy statements, as well as their form and content, we see a picture that deviates in various ways from theoretical observations. With a view to the intention of the European Commission to encourage the development and use of standardised privacy statements, it is important that the empirical research appears to show that industry-level pressure has an effect as regards the use of privacy statements.

As regards the third research question, it is relevant that various agencies point to the importance of transparency and accountability in relation to processing personal data. Thus the European Commission has made it clear in its plans for revising the Privacy Directive that it will place greater emphasis on the principles of transparency and accountability than in the past. Privacy statements appear per se to be a very practical tool to achieve both these principles. Empirical research has, however, demonstrated that the reality is quite different. In any event, the privacy statements that were researched do not offer the desired transparency. Moreover, it turns out that the importance of the transparency that is being

promoted is not being reflected in practice, while at the same time the yardstick being promoted through the principle of accountability aimed at by the European Commission is not complied with either.
If privacy statements are actually going to mean something as regards transparency and accountability, then this research shows that it is necessary to take account of at least the following aspects:

1. The title, traceability and accessibility of the privacy statement;
2. The form of the privacy statement; and
3. The content, readability and comprehensibility of the privacy statement.

It is also significant that research in the United States into the use of privacy statements appears to support the hypothesis that the required degree of transparency can be achieved more effectively by developing standardised privacy statements. The empirical research also seems to show that pressure at industry level as regards use of privacy statements has an effect. The research in the United States moreover seems to show that pressure by the legislators for the use of privacy statements has an effect on the development of privacy statements. Finally, the European Commission is also considering emphasising the development and use of standardised privacy statements. In short, encouraging the development and use of standardised privacy statements is, if one bases one's reasoning on transparency and accountability, something which certainly needs to be taken into account during the future development of transparency as regards processing of personal data and therefore the use of privacy statements.

On the basis of this observation, chapter 6 investigates how standardised privacy statements could be developed throughout the entire EU. The point of departure taken here – also with a view to the proposal to amend the Privacy Directive which appeared at the start of 2012 – is that the main aspects of a standardised privacy statement should be developed at EU level, and that the industry-based implementation should take place at national level. We conclude that the initiative to develop generally standardised privacy statements is a responsibility for European legislators. The industry-wide implementation should then take place at national level by means of self-regulatory pressure. Lastly, industry organisations could require compulsory use by their members of standardised industry-wide privacy statements.

Bijlage A1: Overzicht online verzekeraars

www.abnamro.nl
www.klaverblad.nl
www.centraalbeheer.nl
www.kruidvat.nl
www.aegon.nl
www.lancyr.nl
www.agisweb.nl
www.menzis.nl
www.allsecure.nl
www.mondial-assistance.nl
www.anderzorg.nl
www.moneyou.nl
www.anwb.nl
www.nationaalspaarfonds.nl
www.arag.nl
www.navk.nl
www.asrverzekeringen.nl
www.netpolis.nl
www.azivo.nl
www.ohra.nl
www.cz.nl
www.ozf.nl
www.das.nl
www.polisdirect.nl
www.defriesland.nl
www.premio.nl
www.denationale.nl
www.prolife.nl
www.dela.nl
www.salland.nl
www.deltalloyd.nl
www.snsbank.nl
www.ditzo.nl
www.splendis.nl
www.dsw.nl
www.stadholland.nl
www.europeesche.nl

www.takecarenow.nl
www.facultatieve-verzekeringen.nl
www.trias.nl
www.fbto.nl
www.unigarant.nl
www.feestzeker.nl
www.unive.nl
www.firstowner.nl
www.vgz.nl
www.groeneland.nl
www.zilverenkruis.nl
www.hema.nl
www.zorgenzekerheid.nl
www.ineas.nl
www.proteqdierenzorg.nl
www.ing.nl
www.trouwzeker.nl
www.inshared.nl
www.oriondirect.nl
www.iza.nl

Bijlage A2: Overzicht online reiswinkels

www.aanzee.com
www.arke.nl
www.oad.nl
www.beachmasters.nl
www.basic-travel.com/nl
www.one2gethertravel.nl
www.bellavakanza.nl
www.beter-uit.nl
www.palmboom.nl
www.belvilla.nl
www.bex.nl
www.peterlanghout.nl
www.bizztravel.nl
www.chalet.nl
www.pharosreizen.nl
www.bookfriesland.nl
www.effeweg.nl
www.rpholidays.nl
www.budgetair.nl
www.clubskisportief.nl
www.vakantiexperts.nl
www.camelot.nl
www.corendon.nl
www.shoestring.nl
www.chaletsplus.com
www.cruisetravel.nl
www.skichalets.nl
www.cheaptickets.nl
www.djoser.nl
www.skytours.nl
www.cruisetarieven.nl
www.d-reizen.nl
www.snoeyink.nl
www.beaches.nl
www.eurocamp.nl
www.sudtours.nl
www.elizawashere.nl

www.keycamp.nl
www.sundirect.nl
www.elmarreizen.nl
www.fastminute.nl
www.sunski.nl
www.eurorelais.nl
www.flextravel.nl
www.thomascook.nl
www.ferio.nl
www.fox.nl
www.tsjechoreizen.nl
www.gogo.nl
www.globereisburo.nl
www.toerkoop.nl
www.hurenengenieteninspanje.nl
www.kidsworldclub.nl
www.topictravel.nl
www.husk.nl
www.gomundo.nl
www.totalstay.nl
www.jiba.nl
www.goodbookers.nl
www.skihorizon.nl
www.julesvillas.nl
www.happyhome.nl
www.vacanceselect.nl
www.snowtrex.nl
www.hollandinternational.nl
www.vacansoleil.nl
www.sunweb.nl
www.hotels.com
www.vakantiediscounter.nl
www.tnfsh.nl
www.hotelspecials.nl
www.skistuds.nl
www.vacancesprovence.nl
www.kilroyworld.nl
www.vakantiekoorts.nl
www.vaya.nl
www.kras.nl

www.vannood.nl
www.villaxl.com
www.lacasita.com
www.vandervalkvakanties.nl
www.vliegtickets.nl
www.landal.nl
www.vrijuit.nl
www.vliegwinkel.nl
www.marysol.nl
www.worldticketcenter.nl
www.breakloose.nl
www.riksjaonline.nl
www.hotelaanbiedingen.nl
www.x-travel.nl
www.neckermann.nl
www.captaincruise.nl
www.zillertal-reizen.nl
www.niletravel.nl
www.solmar.nl
www.zoweg.nl
www.nosun.nl
www.snp.nl
www.ebookers.nl

Bijlage A3: Overzicht online kledingwinkels

www.tom-tailor.nl
www.dressesonly.nl
www.jitsefashion.nl
www.wehkamp.nl
www.eukids.nl
www.jolinejolink.com
www.acmetrendz.com
www.easyunderwear.nl
www.kaia.nl
www.aktiesport.nl
www.esprit.nl
www.kidscotton.com
www.annaki.nl
www.fairkids.nl
www.kinderkleding.nl
www.antonio-verago.nl
www.fashionmanor.eu
www.kindervoordeel.nl
www.heine-shop.nl
www.fashionmania.nl
www.kleding-heren.nl
www.babybutt.nl
www.females.nl
www.kleertjes.com
www.babyandmom.nl
www.freshlabelz.nl
www.kleren.com
www.babysbest.nl
www.freshcotton.com
www.klingel.nl
www.badjasparadijs.nl
www.gaastraproshop.com
www.kymare-eshop.com
www.bewareforkids.nl
www.gabberwear.nl
www.ladress.com/nl
www.bienvenu.nl

www.gardenoffashion.nl
www.label54.nl
www.billy-lilly.nl
www.geboortewinkel.nl
www.sokshop.nl
www.blomma.nl
www.give2you.nl
www.luxedassen.nl
www.bolifestyle.nl
www.goodmoodkid.nl
www.mannennu.nl
www.bodydreams.nl
www.greenjump.nl
www.mcgregorstore.com/nl
www.bodyplein.nl
www.grote-cupmaten.nl
www.melkofpuur.nl
www.bombersonline.com
www.haburi.nl
www.menatwork.nl
www.bonaparte.nl
www.happybee.nl
www.mensocks.nl
www.boxershorts.nl
www.hipvoordeheb.nl
www.merkfashiononline.nl
www.brickwear.nl
www.honeymoonwebshop.nl
www.merkkleding.nl
www.broekies.nl
www.hunkemoller.nl
www.mieniemie.nl
www.brunottishop.com/nl/
www.izilivinwebshop.com
www.modeon.nl
www.camouflagekledingwinkel.nl
www.ietjecompany.nl
www.modevoorkids.nl
www.capecomfort.com
www.intimobella.nl

www.mooiemerken.nl
www.chickiesbinkies.nl
www.jeansandfashion.com
www.mumsmarket.nl
www.dassenonline.nl
www.italian-design.nl
www.neck.nl
www.davidandthomas.nl
www.puntoitaliano.nl
www.otto.nl
www.denimtrend.nl
www.jeansonline.nl
www.overhemdenstore.nl
www.derycke.nl
www.lannis.nl
www.peppadewkids.nl
www.dimenno.nl
www.jetsbabystore.nl
www.perfectlybasics.nl
www.directondergoed.nl
www.jimmyandjill.com
www.score.nl
www.dress-for-less.nl

Bijlage B: Vragenlijst empirisch onderzoek

1. Heeft de online winkel een privacyverklaring op zijn website opgenomen?

2. Wat is de verschijningsvorm van de privacyverklaring?

3. Wordt de privacyverklaring in getrapte vorm gegeven?

4. Wat is de benaming van de button van de hyperlink of vaste pop up scherm?

5. Is de button van de hyperlink op de home pagina weergegeven, en zo ja,
wat is de positie van de button?

6. Is de button van de hyperlink zichtbaar zonder dat er gescrolled hoeft te worden?

7. Is de button van het vaste pop-up scherm op de home pagina weergegeven, en zo ja,
wat is de positie van de button?

8. Is de button van het vaste pop-up scherm zichtbaar zonder dat er gescrolled hoeft te worden?

9. Kan de betrokkene de privacyverklaring opslaan?

10. Wordt de identiteit van de verantwoordelijke vermeld?

11. Wordt het doel van de verwerking vermeld?

12. Wordt er vermeld dat de verantwoordelijke belang hecht aan de privacy van de betrokkene?

13. Wordt er vermeld dat de verantwoordelijke aan de hand van de privacyverklaring wil voldoen
aan zijn informatieplicht die hij heeft op grond van de Wbp?

14. Wordt het fysieke adres van de verantwoordelijke vermeld?

15. Wordt het elektronische adres van de verantwoordelijke vermeld?

16. Wordt vermeld of verduidelijkt dat er bijzondere gegevens worden verwerkt?

17. Wordt vermeld of het verstrekken van bepaalde informatie verplicht of facultatief is?

18. Wordt vermeld voor welke ontvangers of categorieën van ontvangers binnen de organisatie van de verantwoordelijke de verzamelde persoonsgegevens bestemd is?

19. Wordt vermeld hoe lang de bewaartermijn is van de verzamelde persoonsgegevens?

20. Wordt melding gemaakt van het recht van de betrokkene op toegang tot de persoonsgegevens?

21. Wordt melding gemaakt van het recht van de betrokkene op rectificatie van de persoonsgegevens?

22. Wordt melding gemaakt van het recht van de betrokkene op verwijdering van de persoonsgegevens?

23. Wordt melding gemaakt van het recht van de betrokkene om, afhankelijk van de situatie, zich te verzetten tegen de verwerking van persoonsgegevens?

24. Wordt vermeld of er beveiligingsmaatregelen zijn getroffen om bijvoorbeeld de authenticiteit van de website en/of de integriteit en vertrouwelijkheid van de via de website overgedragen persoonsgegevens te waarborgen?

25. Wordt vermeld dat de verwerking is gemeld bij het Cbp?

26. Wordt vermeld dat de verwerking is gemeld bij een functionaris voor de gegevensbescherming?

27. Wordt melding gemaakt van de naam van de afdeling of functionaris tot wie de betrokkene zich moet wenden om zijn rechten uit te oefenen?

28. Wordt de naam vermeld van de afdeling of functionaris die verantwoordelijk is voor het beantwoorden van vragen betreffende de bescherming van persoonsgegevens?

29. Wordt vermeld of persoonsgegevens al dan niet aan derden worden verstrekt?

30. Wordt vermeld of persoonsgegevens aan derden worden verstrekt op grond van een wettelijke plicht?

31. Worden er derden benoemd?

32. Wordt vermeld dat de persoonsgegevens, al dan niet mogelijk, naar een derde in het buitenland worden verstrekt?

33. Wordt vermeld dat derden de vertrouwelijkheid en/of beveiliging van de persoonsgegevens garanderen?

34. Wordt melding gemaakt dat de verantwoordelijke al dan niet gebruik maakt van cookies?

35. Wordt in de privacyverklaring melding gemaakt of er derden betrokken zijn geweest bij de totstandkoming van de inhoud van de privacyverklaring?

36. Wordt in de privacyverklaring verklaard of de verantwoordelijke gebonden is, dan wel zich gebonden acht, aan een gedragscode?

37. Indien ja, kan de betrokkene kennisnemen van de inhoud van die gedragscode en op welke wijze?

38. Wordt gerefereerd aan of gedoeld op de Gedragscode Financiële Instellingen?

39. Wordt in de privacyverklaring vermeld dat de betrokkene akkoord gaat met de inhoud van de privacyverklaring zodra hij zijn persoonsgegevens verstrekt?

40. Wordt in de privacyverklaring vermeld dat de betrokkene akkoord gaat met de inhoud van de privacyverklaring zodra hij zich op de website van de verantwoordelijke begeeft?

41. Wordt in de privacyverklaring vermeld dat de betrokkene, al dan niet voor specifieke verwerkingen, toestemming moet geven of heeft gegeven aan de verantwoordelijke om zijn persoonsgegevens te mogen verwerken?

42. Wordt vermeld dat de betrokkene zijn toestemming te alle tijden kan intrekken?

43. Wordt in de privacyverklaring verklaard of er wel of geen overeenkomt tussen de verantwoordelijke en de betrokkene tot stand komt?

44. Wordt melding gemaakt welke (rechts)maatregelen de betrokkene kan treffen indien de verantwoordelijke tekortschiet in het verwerken van de persoonsgegevens of onrechtmatig handelt jegens de betrokkene?

45. Behoudt de verantwoordelijke zich het recht voor om de inhoud van de privacyverklaring eenzijdig te wijzigen?

46. Indien ja, op welke wijze wordt de betrokkene geïnformeerd in geval van wijzigingen van de privacyverklaring?

47. Zijn er, naast de privacyverklaring, elektronische algemene voorwaarden?

48. Zijn er in de algemene voorwaarden bepalingen opgenomen die zien op de verwerking van persoonsgegevens?

49. Wordt in de algemene voorwaarden de identiteit van de verantwoordelijke vermeld?

50. Wordt de identiteit van de verantwoordelijke elders op de website vermeld?

51. Wordt in de algemene voorwaarden het doel van de verwerking vermeld?

52. Wordt het doel van de verwerking elders op de website vermeld?

Ten behoeve online verzekeraars

53. Is de verantwoordelijke lid van het Verbond van Verzekeraars of NVB?

54. Is de verantwoordelijke lid van Thuiswinkel.org?

55. Wordt vermeld of de verantwoordelijke gebruik maakt van CIS?

56. Wordt vermeld op welke wijze de verantwoordelijke het CIS gebruikt?

57. Wordt verwezen naar de privacyverklaring van de CIS?

58. Wordt de verhouding tussen de privacyverklaring en die van de CIS verduidelijkt?

59. Wordt vermeld dat de leden van CIS onderling gegevens uitwisselen?

Ten behoeve van online reiswinkels

60. Is de verantwoordelijke lid van de ANVR?

61. Is de verantwoordelijke lid van Thuiswinkel.org?

Ten behoeve van online kledingwinkels

62. Is de verantwoordelijke lid van Thuiswinkel.org?

Bijlage C1: Tabellen segment verzekeringen

Onderling statistisch significante verschillen met betrekking tot het wel of niet lid zijn van de online verzekeraar van de belangenorganisatie Verbond van Verzekeraars.

	Totaal		Lid Verbond van Verzekeraars		Geen lid	
Wordt in de AV de identiteit van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	1	5,0	1	33,3	0	0,0
Ja, de naam van de natuurlijke persoon	0	0,0	0	0,0	0	0,0
Ja, de statutaire naam van de rechtspersoon	2	10,0	0	0,0	2	11,8
Ja, de handelsnaam	17	85,0	2	66,7	15	88,2
			Pearson $\chi 2$= 6,2 df=2; p<.05			

	Totaal		Lid Verbond van Verzekeraars		Geen lid	
Wordt het elektronische adres van de verantwoordelijke elders op de website vermeld?	n	%	n	%	n	%
Nee	25	64,1	14	82,4	11	50,0
Ja	14	35,9	3	17,6	11	50,0
			Pearson $\chi 2$= 4,4 df=1; p<.05			

	Totaal		Lid Verbond van Verzekeraars		Geen lid	
Wordt de identiteit van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	1	1,9	0	0,0	1	3,4
Ja, de naam van de natuurlijke persoon	0	0,0	0	0,0	0	0,0
Ja, de statutaire naam van de rechtspersoon	32	59,3	22	88,0	10	34,5
Nee, maar wel de handelsnaam	21	38,9	3	12,0	18	62,1
			Pearson χ^2= 16,0 df=1; p<.001			

	Totaal		Lid Verbond van Verzekeraars		Geen lid	
Wordt vermeld en/of verduidelijkt dat er bijzondere gegevens worden verwerkt?	n	%	n	%	n	%
Nee	17	31,5	3	12,0	14	48,3
Ja, er worden geen bijzondere gegevens verwerkt	0	0,0	0	0,0	0	0,0
Ja, er worden geen bijzondere gegevens verwerkt, tenzij met toestemming betrokkene	1	1,9	1	4,0	0	0,0
Ja, medische gegevens	12	22,2	2	8,0	10	34,5
Ja, strafrechtelijke gegevens	5	9,3	3	12,0	2	6,9
Ja, zowel medische als strafrechtelijke gegevens	18	33,3	15	60,0	3	10,3
Ja, maar niet nader verduidelijkt	1	1,9	1	4,0	0	0,0
			Pearson χ^2= 22,5 df=5; p<.001			

	Totaal		Lid Verbond van Verzekeraars		Geen lid	
Wordt vermeld of persoonsgegevens aan derden worden verstrekt?	n	%	n	%	n	%
Nee	24	44,4	16	64,0	8	27,6
Ja	30	55,6	9	36,0	21	72,4
			Pearson χ^2= 7,2 df=1; p<.01			

	Totaal		Lid Verbond van Verzekeraars		Geen lid	
Wordt vermeld of persoonsgegevens aan derden worden verstrekt op grond van een wettelijke plicht?	n	%	n	%	n	%
Nee	38	70,4	21	84,0	17	58,6
Ja	16	29,6	4	16,0	12	41,4
			Pearson χ^2= 4,1 df=1; p<.05			

Bijlage C2: Tabellen segment verzekeringen

Onderling statistisch significante verschillen met betrekking tot het wel of niet lid zijn van de online verzekeraar van de belangenorganisatie Thuiswinkel.org.

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wat is de verschijningsvorm van de privacyverklaring?	n	%	n	%	n	%
Hyperlink	0	0,0	0	0,0	0	0,0
Pop up scherm die verschijnt na een handmatige klik	51	94,4	18	85,7	33	100
Vast tekstvensters	3	5,6	3	14,3	0	0,0
Pop up scherm die automatisch verschijnt	0	0,0	0	0,0	0	0,0
Anders	0	0,0	0	0,0	0	0,0
			Pearson χ^2=5,0 df=1; p<.05			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt vermeld dat de verwerking is gemeld bij de FG?	n	%	n	%	n	%
Nee	47	87,0	15	71,4	32	97,0
Ja	7	13,0	6	28,6	1	3,0
			Pearson χ^2=7,4 df=1; p<.01			

Bijlage C3: Tabellen segment verzekeringen

Onderling statistisch significante verschillen met betrekking tot het wel of niet lid zijn van de online verzekeraar van de belangenorganisatie Verbond van Verzekeraars, Thuiswinkel.org of van beiden.

Identiteit van de verantwoordelijke uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Wordt de identiteit van de verantwoordelijke vermeld?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	0	(0,0)	0	(0,0)	1	(8,3)	0	(0,0)	1	(1,9)
Ja, de naam van de natuurlijke persoon	0	(0,0)	0	(0,0)	0	(0,0)	0	(0,0)	0	(0,0)
Ja, de statutaire naam van de rechtspersoon	4	(23,5)	13	(81,3)	6	(50,0)	9	(100,0)	32	(59,3)
Ja, de handelsnaam	13	(76,5)	3	(18,8)	5	(41,7)	0	(0,0)	21	(38,9)
Totaal	17		16		12		9		54	

Vermelding recht op toegang uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Wordt melding gemaakt van het recht van de betrokkene op toegang tot de persoonsgegevens?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	9	(52,9)	3	(18,8)	2	(16,7)	1	(11,1)	15	(27,8)
Ja	8	(47,1)	13	(81,3)	10	(83,3)	8	(88,9)	39	(72,2)
Totaal	17		16		12		9		54	

Vermelding fysieke adres van de verantwoordelijke uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)

Wordt het fysieke adres van de verantwoordelijke vermeld?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	16	(94,1)	14	(87,5)	7	(58,3)	9	(100)	46	(85,2)
Ja	1	(5,9)	2	(12,5)	5	(41,7)	0	(0,0)	8	(14,8)
Totaal	17		16		12		9		54	

Vermelding Cbp-melding uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)

Wordt vermeld dat de verwerking is gemeld bij het Cbp?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	3	(17,6)	7	(43,8)	9	(75,0)	2	(22,2)	21	(38,9)
Ja, inclusief het nummer van registratie	3	(17,6)	5	(31,3)	1	(8,3)	1	(11,1)	10	(18,5)
Ja, zonder nummer van registratie	11	(64,7)	4	(25,0)	2	(16,7)	6	(66,7)	23	(42,6)
Totaal	17		16		12		9		54	

Vermelding verwerking bijzondere gegevens uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)

Wordt vermeld of verduidelijkt dat er bijzondere gegevens worden verwerkt?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	7	(41,2)	3	(18,8)	7	(58,3)	0	(0,0)	17	(31,5)
Ja, er worden geen bijzondere gegevens verwerkt	0	(0,0)	0	(0,0)	0	(0,0)	0	(0,0)	0	(0,0)
Ja, er worden geen bijzondere gegevens verwerkt, tenzij met toestemming betrokkene	0	(0,0)	1	(6,3)	0	(0,0)	0	(0,0)	1	(1,9)

Ja, medische gegevens	8	(47,1)	2	(12,5)	2	(16,7)	0	(0,0)	12	(22,2)
Ja, strafrechtelijke gegevens	0	(0,0)	1	(6,3)	2	(16,7)	2	(22,2)	5	(9,3)
Ja, zowel medische als strafrechtelijke gegevens	2	(11,8)	8	(50,0)	1	(8,3)	7	(77,8)	18	(33,3)
Ja, maar niet nader verduidelijkt	0	(0,0)	1	(6,3)	0	(0,0)	0	(0,0)	1	(1,9)
Totaal	17		16		12		9		54	

Verstrekking gegevens aan derden uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)

Wordt vermeld of persoonsgegevens al dan niet aan derden worden verstrekt?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	4	(23,5)	12	(75,0)	4	(33,3)	4	(44,4)	24	(44,4)
Ja	13	(76,5)	4	(25,0)	8	(66,7)	5	(55,6)	30	(55,6)
Totaal	17		16		12		9		54	

Vermelding dat verantwoordelijke gebruik maakt van CIS uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)

Wordt vermeld of de verantwoordelijke gebruik maakt van CIS?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	15	(88,2)	5	(31,3)	9	(75,0)	0	(0,0)	29	(53,7)
Ja	2	(11,8)	11	(68,8)	3	(25,0)	9	(100,0)	25	(46,3)
Totaal	17		16		12		9		54	

Bijlage D: Tabellen Stichting Centraal Informatie Systeem

	Verzekeringen	
Wordt vermeld of de verantwoordelijke gebruik maakt van CIS?	n	%
Nee	29	53,7
Ja	25	46,3

	Verzekeringen	
Wordt vermeld op welke wijze de verantwoordelijke het CIS gebruikt?	n	%
Nee	2	8,0
Raadplegen van persoonsgegevens van de betrokkene	23	92,0
Verstrekken van (persoons)gegevens aan het CIS	0	0,0
Raadplegen en verstrekken van (persoons)gegevens	0	0,0

	Verzekeringen	
Wordt verwezen naar de privacyverklaring van CIS?	n	%
Nee	1	4,0
Ja	24	96,0

	Verzekeringen	
Wordt de verhouding tussen de privacyverklaring en die van CIS verduidelijkt?	n	%
Nee	25	100
Ja	0	0,0

	Verzekeringen	
Wordt vermeld dat de leden van CIS onderling gegevens uitwisselen?	n	%
Nee	13	52,0
Ja	12	48,0

Bijlage E1: Tabellen segment reizen

Onderling statistisch significante verschillen met betrekking tot het wel of niet lid zijn van de online reiswinkel van de belangenorganisatie ANVR.

	Totaal		Lid ANVR		Geen lid	
Wordt er vermeld dat de verantwoordelijke belang hecht aan de privacy van de betrokkene?	n	%	n	%	n	%
Nee	15	21,1	7	14,0	8	38,1
Ja	56	78,9	43	86,0	13	61,9
			Pearson χ^2=5,2 df=1; p<.05			

Bijlage E2: Tabellen segment reizen

Onderling statistisch significante verschillen met betrekking tot het wel of niet lid zijn van de online reiswinkel van de belangenorganisatie Thuiswinkel.org.

	Totaal		Lid Thuiswinkel.org		Geen lid	
Heeft de online winkel een privacyverklaring op zijn website opgenomen?	n	%	n	%	n	%
Nee	29	29,0	1	2,6	28	45,9
Ja	71	71,0	38	97,4	33	54,1
			Pearson χ^2= 21,7 df=1; p<.001			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt in de AV het fysieke adres van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	55	67,1	11	34,4	44	88,0
Ja	27	32,9	21	65,6	6	12,0
			Pearson χ^2= 25,4 df=1; p<.001			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt in de AV het elektronische adres van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	35	63,6	1	12,5	34	72,3
Ja	20	36,4	7	87,5	13	27,7
			Pearson χ^2= 10,6 df=1; p<.01			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt het fysieke adres van de verantwoordelijke elders op de website vermeld?	n	%	n	%	n	%
Nee	9	24,3	0	0,0	9	34,6
Ja	28	75,7	11	100	17	65,4
			Pearson χ^2= 5,0 df=1; p<.05			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt de identiteit van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	1	1,4	0	0,0	1	3,0
Ja, de naam van de natuurlijke persoon	0	0,0	0	0,0	0	0,0
Ja, de statutaire naam van de rechtspersoon	18	25,4	5	13,2	13	39,4
Nee, maar wel de handelsnaam	52	73,2	33	86,8	19	57,6
			Pearson χ^2= 8,0 df=2; p<.05			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt het elektronische adres van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	31	43,7	7	18,4	24	72,7
Ja	40	56,3	31	81,6	9	27,3
			Pearson χ^2= 21,2 df=1; p<.001			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt vermeld of er beveiligingsmaatregelen zijn getroffen om bijvoorbeeld de authenticiteit van de website en/of de integriteit en vertrouwelijkheid van de via de site overgedragen persoonsgegevens te waarborgen?	n	%	n	%	n	%
Nee	41	57,7	15	39,5	26	78,8
Ja	30	42,3	23	60,5	7	21,2
			Pearson χ^2= 11,2 df=1; p<.01			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt melding gemaakt van het recht van de betrokkene op toegang tot de persoonsgegevens?	n	%	n	%	n	%
Nee	42	59,2	14	36,8	28	84,8
Ja	29	40,8	24	63,2	5	15,2
			Pearson χ^2= 16,8 df=1; p<.001			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt melding gemaakt van het recht van de betrokkene om, afhankelijk van de situatie, zich te verzetten tegen de verwerking van persoonsgegevens?	n	%	n	%	n	%
Nee	21	29,6	6	15,8	15	45,5
Ja	50	70,4	32	84,2	18	54,5
			Pearson χ^2= 7,5 df=1; p<.01			

Bijlage E3: Tabellen segment reizen

Onderling statistisch significante verschillen met betrekking tot het wel of niet lid zijn van de online reiswinkel van de belangenorganisatie ANVR, Thuiswinkel.org of van beiden.

Op website opgenomen privacyverklaring uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Heeft de online winkel een privacyverklaring op zijn website opgenomen?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	14	(63,6)	14	(35,9)	0	(0,0)	1	(3,8)	29	(29,0)
Ja	8	(36,4)	25	(64,1)	13	(100,0)	25	(96,2)	71	(71,0)
Totaal	22		39		13		26		100	

Vermelding identiteit van de verantwoordelijke uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Wordt de identiteit van de verantwoordelijke vermeld?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	0	(0,0)	1	(4,0)	0	(0,0)	0	(0,0)	1	(1,4)
Ja, de naam van de natuurlijke persoon	0	(0,0)	0	(0,0)	0	(0,0)	0	(0,0)	0	(0,0)
Ja, de statutaire naam van de rechtspersoon	1	(12,5)	12	(48,0)	2	(15,4)	3	(12,0)	18	(25,4)
Ja, de handelsnaam	7	(87,5)	12	(48,0)	11	(84,6)	22	(88,0)	52	(73,2)
Totaal	8		25		13		25		71	

Vermelding recht op toegang uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Wordt melding gemaakt van het recht van de betrokkene op toegang tot de persoonsgegevens?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	5	(62,5)	23	(92,0)	6	(46,2)	8	(32,0)	42	(59,2)
Ja	3	(37,5)	2	(8,0)	7	(53,8)	17	(68,0)	29	(40,8)
Totaal	8		25		13		25		71	

Vermelding recht van verzet uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Wordt melding gemaakt van het recht van de betrokkene om, afhankelijk van de situatie, zich te verzetten tegen de verwerking van persoonsgegevens?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	3	(37,5)	12	(48,0)	4	(30,8)	2	(8,0)	21	(29,6)
Ja	5	(62,5)	13	(52,0)	9	(69,2)	23	(92,0)	50	(70,4)
Totaal	8		25		13		25		71	

Vermelding elektronische adres van de verantwoordelijke uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Wordt het elektronische adres van de verantwoordelijke vermeld?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	5	(62,5)	19	(76,0)	3	(23,1)	4	(16,0)	31	(43,7)
Ja	3	(37,5)	6	(24,0)	10	(76,9)	21	(84,0)	40	(56,3)
Totaal	8		25		13		25		71	

Vermelding Cbp-melding uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Wordt vermeld dat de verwerking is gemeld bij het Cbp?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	6	(75,0)	16	(64,0)	9	(69,2)	13	(52,0)	44	(62,0)
Ja, inclusief het nummer van registratie	1	(12,5)	4	(16,0)	3	(23,1)	0	(0,0)	8	(11,3)
Ja, zonder nummer van registratie	1	(12,5)	5	(20,0)	1	(7,7)	12	(48,0)	19	(26,8)
Totaal	8		25		13		25		71	

Vermelding FG-melding uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Wordt vermeld dat de verwerking is gemeld bij een functionaris voor de gegevensbescherming?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	17	(100,0)	15	(93,7)	8	(66,7)	7	(77,8)	47	(87,0)
Ja	0	(0,0)	1	(6,3)	4	(33,3)	2	(22,2)	7	(13,0)
Totaal	17		16		12		9		54	

Vermelding beveiligingsmaatregelen uitgesplitst naar lidmaatschap (met tussen haakjes de percentages)										
Wordt vermeld of er beveiligingsmaatregelen zijn getroffen om bijvoorbeeld de authenticiteit van de website en/of de integriteit en vertrouwelijkheid van de via de website overgedragen persoonsgegevens te waarborgen?	Lidmaatschap								totaal	
	nergens lid van		alleen lid van de branche		alleen lid van TW		lid van de branche en van TW			
Nee	6	(75,0)	20	(80,0)	5	(38,5)	10	(40,0)	41	(57,7)
Ja	2	(25,0)	5	(20,0)	8	(61,5)	15	(60,0)	30	(42,3)
Totaal	8		25		13		25		71	

Bijlage F: Tabellen segment kleding

Onderling statistisch significante verschillen met betrekking tot het wel of niet lid zijn van de online kledingwinkel van de belangenorganisatie Thuiswinkel.org.

	Totaal		Lid Thuiswinkel.org		Geen lid	
Heeft de online winkel een privacyverklaring op zijn website opgenomen?	n	%	n	%	n	%
Nee	29	29,0	0	0,0	29	37,2
Ja	71	71,0	22	100,0	49	62,8
			Pearson $\chi 2$= 11,5 df=1; p<.001			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Kan de betrokkene de privacyverklaring opslaan?	n	%	n	%	n	%
Nee	64	90,1	16	72,7	48	98,0
Ja	7	9,9	6	27,3	1	2,0
			Pearson $\chi 2$= 10,9 df=1; p<.001			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Zijn er bepalingen opgenomen die zien op de verwerking van persoonsgegevens?	n	%	n	%	n	%
Nee	52	54,2	17	77,3	35	47,3
De bepalingen zijn materieel van aard	38	39,6	5	22,7	33	44,6
Er wordt bepaald dat de privacyverklaring onderdeel uit maakt van de algemene voorwaarden	0	0,0	0	0,0	0	0,0
Er wordt bepaald dat de privacyverklaring van toepassing is in geval van verwerkingen van persoonsgegevens, maar	6	6,3	0	0,0	6	8,1

de (mogelijke) verhouding tussen elektronische algemene voorwaarden en de privacyverklaring wordt niet verduidelijkt						
			Pearson $\chi 2$= 6,6 df=2; p<.05			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt in de AV het fysieke adres van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	34	45,3	1	10,0	33	50,8
Ja	41	54,7	9	90,0	32	49,2
			Pearson $\chi 2$= 5,8 df=1; p<.05			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt de identiteit van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	6	8,5	0	0,0	6	12,2
Ja, de naam van de natuurlijke persoon	0	0,0	0	0,0	0	0,0
Ja, de statutaire naam van de rechtspersoon	15	21,1	10	45,5	5	10,2
Nee, maar wel de handelsnaam	50	70,4	12	54,5	28	77,6
			Pearson $\chi 2$= 12,8 df=2; p<.01			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt melding gemaakt van het recht van de betrokkene op toegang tot de persoonsgegevens?	n	%	n	%	n	%
Nee	30	42,3	4	18,2	26	53,1
Ja	41	57,7	18	81,8	23	46,9
			Pearson $\chi 2$= 7,6 df=1; p<.01			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt het fysieke adres van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	49	69,0	10	45,5	39	79,6
Ja	22	31,0	12	54,5	10	20,4
			Pearson $\chi 2$= 8,3 df=1; p<.01			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt het elektronische adres van de verantwoordelijke vermeld?	n	%	n	%	n	%
Nee	35	49,3	6	27,3	29	59,2
Ja	36	50,7	16	72,7	20	40,8
			Pearson $\chi 2$= 6,2 df=1; p<.05			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt melding gemaakt dat de website gebruik maakt van cookies?	n	%	n	%	n	%
Nee	24	33,8	2	9,1	22	44,9
Ja	47	66,2	20	90,9	27	55,1
			Pearson $\chi 2$= 8,7 df=1; p<.01			

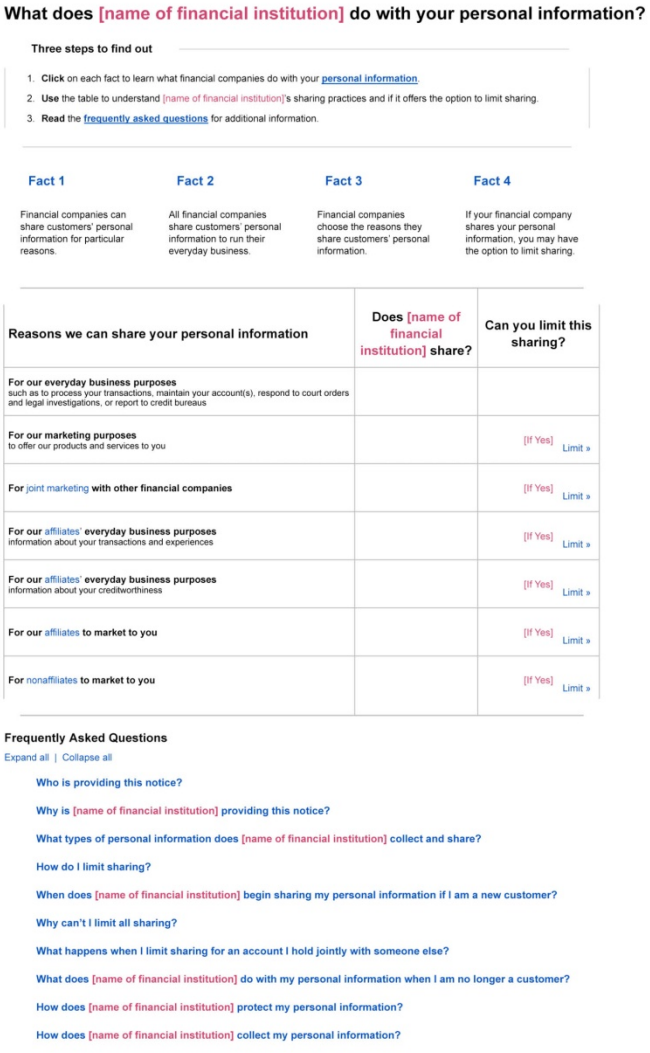
	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt melding gemaakt van de naam en adres tot wie de betrokkene zich moet wenden om zijn rechten uit te oefenen?	n	%	n	%	n	%
Nee	36	50,7	7	31,8	29	59,2
Ja, de Functionaris Gegevensbescherming	0	0,0	0	0,0	0	0,0
Ja, de naam van de privacy officer / coördinator	0	0,0	0	0,0	0	0,0
Ja, de naam van de afdeling	35	49,3	15	68,2	20	40,8
			Pearson $\chi 2$= 4,5 df=1; p<.05			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt de naam vermeld van de afdeling of functionaris die verantwoordelijk is voor het beantwoorden van vragen betreffende de bescherming van persoonsgegevens?	n	%	n	%	n	%
Nee	38	53,5	6	27,3	32	65,3
Ja, de Functionaris Gegevensbescherming	0	0,0	0	0,0	0	0,0
Ja, de naam van de privacy officer / coördinator	0	0,0	0	0,0	0	0,0
Ja, de naam van de afdeling	33	46,5	16	72,7	17	34,7
			Pearson $\chi 2$= 8,8 df=1; p<.01			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Indien ja, op welke wijze wordt de betrokkene geïnformeerd in geval van wijzigingen van de privacyverklaring	n	%	n	%	n	%
De betrokkene dient zelf de privacyverklaring op de website regelmatig te raadplegen	20	60,6	5	35,7	15	78,9
De verantwoordelijke informeert de betrokkene	13	39,4	9	64,3	4	21,1
Wordt niet nader geregeld	0	0,0	0	0,0	0	0,0
			Pearson $\chi 2$= 6,3 df=1; p<.05			

	Totaal		Lid Thuiswinkel.org		Geen lid	
Wordt melding gemaakt welke (rechts)maatregelen de betrokkene kan treffen indien de verantwoordelijke tekortschiet in het verwerken van de persoonsgegevens of onrechtmatig handelt jegens de betrokkene?	n	%	n	%	n	%
Nee	63	88,7	17	77,3	46	93,9
Ja, indienen klacht bij de verantwoordelijke, eventueel gevolgd door een bemiddelings- of klachtenprocedure bij een derde	8	11,3	5	22,7	3	6,1
Ja, rechtstreeks volgen van een bemiddelings- of klachten -procedure bij een derde	0	0,0	0	0,0	0	0,0
Ja, rechtsmaatregelen bij de rechtbank	0	0,0	0	0,0	0	0,0
			Pearson $\chi 2$= 4,2 df=1; p<.05.			

Bijlage G: Web-based financial privacy notice (KCG-Model)



What does [name of financial institution] do with your personal information?

Three steps to find out

1. **Click** on each fact to learn what financial companies do with your personal information.
2. **Use** the table to understand [name of financial institution]'s sharing practices and if it offers the option to limit sharing.
3. **Read** the frequently asked questions for additional information.

Fact 1

Financial companies can share customers' personal information for particular reasons.

Fact 2

All financial companies share customers' personal information to run their everyday business.

Fact 3

Financial companies choose the reasons they share customers' personal information.

Fact 4

If your financial company shares your personal information, you may have the option to limit sharing.

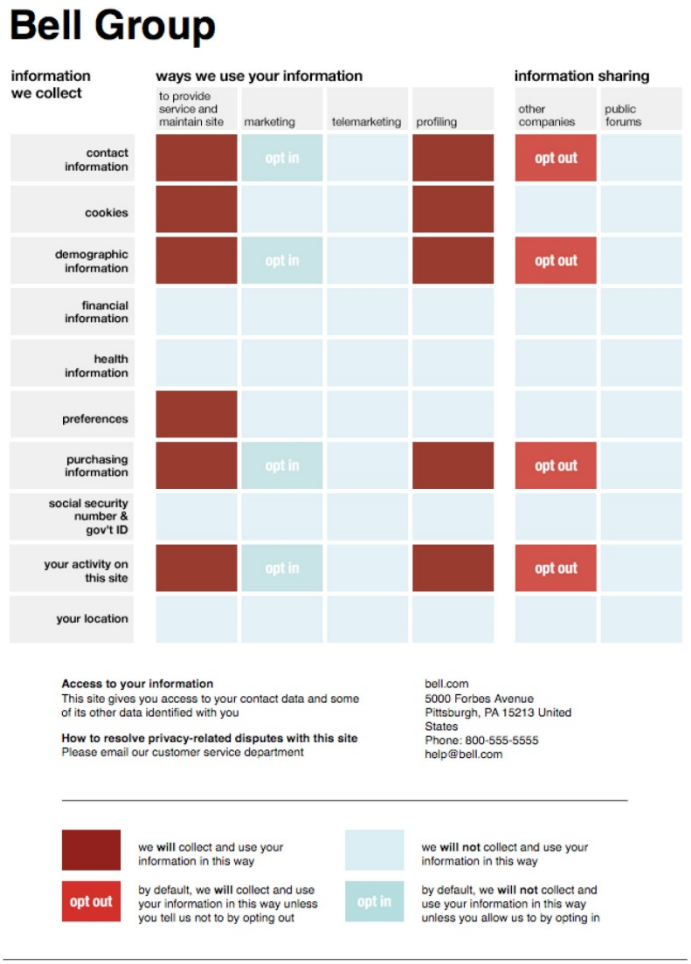
Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes to offer our products and services to you		[If Yes] Limit »
For joint marketing **with other financial companies**		[If Yes] Limit »
For our affiliates' **everyday business purposes** information about your transactions and experiences		[If Yes] Limit »
For our affiliates' **everyday business purposes** information about your creditworthiness		[If Yes] Limit »
For our affiliates **to market to you**		[If Yes] Limit »
For nonaffiliates **to market to you**		[If Yes] Limit »

Frequently Asked Questions

Expand all | Collapse all

- **Who is providing this notice?**
- **Why is [name of financial institution] providing this notice?**
- **What types of personal information does [name of financial institution] collect and share?**
- **How do I limit sharing?**
- **When does [name of financial institution] begin sharing my personal information if I am a new customer?**
- **Why can't I limit all sharing?**
- **What happens when I limit sharing for an account I hold jointly with someone else?**
- **What does [name of financial institution] do with my personal information when I am no longer a customer?**
- **How does [name of financial institution] protect my personal information?**
- **How does [name of financial institution] collect my personal information?**

Bijlage H: Model privacyverklaring Kelly et al.



Bell Group

information we collect	ways we use your information				information sharing	
	to provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	■	opt in		■	opt out	
cookies	■			■		
demographic information	■	opt in		■	opt out	
financial information						
health information						
preferences	■					
purchasing information	■	opt in		■	opt out	
social security number & gov't ID						
your activity on this site	■	opt in		■	opt out	
your location						

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

bell.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@bell.com

■ we **will** collect and use your information in this way

opt out by default, we **will** collect and use your information in this way unless you tell us not to by opting out

we **will not** collect and use your information in this way

opt in by default, we **will not** collect and use your information in this way unless you allow us to by opting in

Definitions

contact information
Contact information may include name, address, phone number, email address, or other online or physical contact information.

cookies
Cookies or mechanisms that perform similar functions. A cookie is a small text file that a website can place on your computer's hard drive to collect information about your activities on the site or to allow the site to remember information about you and your activities.

demographic information
Demographic information may include social and economic categories that apply to you, such as your gender, age, income, or where you are from.

financial information
Financial information may include your accounts, balances, and transactions.

health information
Health information may include data about your medical condition or your interest in health-related topics, services, or products.

marketing
Contacting you through means other than telephone (for example, email or postal mail) to market services or products.

other companies
Most companies share data with business partners who only use your information to provide the services you requested. This cateogory describes sites that share with other companies that use your information beyond fulfilling your requests.

preferences
Preferences may include Information about:

- Your tastes or interests
- Which groups you might be a member of such as religious organizations, trade unions, and political parties

profiling
Collecting information about you in order to:

- Do research and analysis
- Make decisions that directly affect you, such as to display ads based on your activity on the site.

Information that the site collects about you may be linked to an anonymous ID code, or may be linked to your identity.

provide service and maintain site
Collecting information to provide the service you requested, to customize the site for your current visit, to perform web site and system maintenance, or to enhance, evaluate, or otherwise review the site, but without connecting any information to you.

public forums
A public area, such as a bulletin board, chat room, or directory.

purchasing information
Information about your purchases may include the payment methods you used.

social security number & govt ID
Includes government-issued identifiers such as your social security number.

telemarketing
Contacting you by telephone to market services or products.

your activity on this site
Tracking your activity, includes:

- Which pages you visited on this web site and how long you stayed at each page
- Activities you engaged in at this web site, such as your searches and transactions

Messages you sent to the company or post on this site, such as email, bulletin board postings, or chat room conversations

your location
Collect information about your exact geographic location, such as data transmitted by your GPS-enabled device.

Bibliografie

Anthony
S.F. Anthony (Commissioner of the Federal Trade Commission), *The Case for Standardization of Privacy Policy Formats*, Federal Trade Commisson, July 2001.

Antón et al.
A.I. Antón, J.B. Earp & A. Reese, 'Analyzing Website Privacy Requirements Using a Privacy Goal Taxonomy', *Proceedings of the IEEE Joint International Conference on Requirements Engineering (RE'02)*, 2002.

Asser/Hartkamp/Sieburgh
A.S. Hartkamp & C.H. Sieburg, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. Verbintenissenrecht, Algemeen overeenkomstenrecht*, deel 6III', Deventer: Kluwer 2010.

Asser/Vranken
J.B.M. Vranken, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. Algemeen deel*, Deventer: Kluwer 2005.

Australian Government
Australian Government, Office of the Privacy Commissioner, *Privacy Policy*, August 2006.

Baarda & De Goede
D.B. Baarda & M.P.M. de Goede, *Basisboek Methoden en Technieken. Handleiding voor het opzetten en uitvoeren van onderzoek*, Groningen: Stenfert Kroese 2001.

Baarsma et al.
B. Baarsma, F. Felsö, S. van Geffen, J. Mulder & A. Oostdijk, *Zelf doen? Inventarisatiestudie van zelfreguleringsinstrumenten*, Onderzoek in opdracht van het Ministerie van Economische Zaken, Amsterdam: april 2003.

Bakhuysen & Van Emmerik
T. Bakhuysen & M.L. van Emmerik, 'Ongebonden binding. Verwijzing naar soft law-standaarden in uitspraken van het EHRM', *NTMINJCM*, jrg. 35 (2010), nr. 7, p. 827-835.

Beldad
A.D. Beldad, *Trust and information privacy concerns in electronic government* (diss. University of Twente), Enschede 2011.

Beldad et al.
A.D. Beldad, M. de Jong & M.F. Steehouder, 'When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites', *Government Information Quarterly*, Volume 26, Issue 4, 2009, p. 559-566.

Beleidsprogramma Samen werken, samen leven
Beleidsprogramma kabinet Balkenende IV 2007-2011, *Samen werken, samen leven*, Ministerie van Algemene Zaken, juni 2007.

Bendrath
R. Bendrath, 'The Social and Technical Self-Governance of Privacy', in: O. Dilling, M. Herberg & G. Winter, *Responsible Business? Self-Governance and the Law*, Transnational Economic Transactions, Oxford: Hart 2008.

Bennet 2004
C.J. Bennet, 'Privacy Self-Regulation in a Global Economy: A Race to the Top, the Bottom or Somewhere Else?', in: K. Webb, *Voluntary Codes: Private Governance, the Public Interest and Innovation*, Carleton Research Unit for Innovation, Science and Environment, Carleton University, Ottawa, Canada.

Bennet 2010
C.J. Bennet, 'International Privacy Standards: Can Accountability be Adequate?', *Privacy Laws and Business International*, Vol. 106 (August 2010), p. 21-23.

Van den Berg
B. van den Berg, 'Ambient Intelligence: Wat, wie en…waarom?', *Computerrecht* 2010-6, p. 267-272.

Berkvens 2009-a
J.M.A. Berkvens, 'Role of Trade Associations: Data Protection as a Negotiable Issue', in: S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwange & S. Nouwt, *Reinventing Data Protection?*, Dordrecht: Springer 2009, p. 125-129.

Berkvens 2009-b
J.M.A. Berkvens, 'Het verdwijnpunt', *Computerrecht* 2009-3, p. 102.

Berkvens 2011
J.M.A. Berkvens, 'Naar een wereld zonder controllers en processors', *P&I* 2011-5, p. 255-262.

Bigo et al.
D. Bigo, G. González Fuster, E. Guild, P. de Hert, J. Jeandesboz & V. Papakonstantinou, *Towards a New EU Legal Framework for Data Protection and Privacy. Challenges, Principles and the Role of the European Parliament*, European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Brussel, September 2011.

Bitter
C.M. Bitter, 'Privacyprocesrecht', in: J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2007, p. 47-66.

Blok
P. Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlands en Amerikaanse recht* (diss. Tilburg), Den Haag: Boom Juridische uitgevers 2002.

Borking
J.J.F.M. Borking, *Privacyrecht is code, over het gebruik van Privacy Enhancing Technologies* (diss. Leiden), Deventer: Kluwer 2010.

Bovens
Mark Bovens, *Analysing and Assesing Public Accountability. A Conceptual Framework*, European Governance Papers (EUROGOV), No. C-06-01, 2006.

Branchereactie TNO/IViR Rapport
Branchereactie TNO IViR Rapport: 'A bite too big, Dillema's bij de implementatie van de cookiewet in Nederland', brief aan de aan de leden van de Commissie Economische Zaken, 18 maart 2011.

Brouwer-Korf
Adviescommissie Veiligheid en persoonlijke levenssfeer onder voorzitterschap van mevrouw mr. A.H. Brouwer-Korf, *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer*, Den Haag, 2009.

Bruening
P.J. Bruening, 'Accountability: Part Of The International Public Dialogue About Privacy Governance', *Privacy & Security Law*, Bureau of National Affairs, Inc,. USA, 2010.

Buitelaar & Cuijpers
H. Buitelaar & C. Cuijpers, 'De balans tussen veiligheid en privacy. Kanttekeningen bij het standpunt van het kabinet', *NJ* 11 12 2009, afl. 43, nummer 2194, p. 2820-2825.

Cavoukian 2009
A. Cavoukian, S. Taylor & M.E. Abrams, *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices*, November 2009.

Cavoukian 2011
A. Cavoukian, Information and Privacy Commissioner of Ontario, Canada, *Consultation on the Commission's Comprehensive Approach on personal Data Protection in the European Union - Public Authority*, January 13, 2011.

Cbp Brief aan Minister van Justitie
Cbp, Brief aan Minister van Justitie, 7 december 2004, z2004-1086.

Cbp Brief aan Vaste Commissie
Cbp, Brief aan de Leden van de Vaste commissie voor Economische Zaken, Landbouw en Innovatie van de Tweede Kamer der Staten-Generaal, 14 maart 2011.

Cbp Brochure Gedragscodes
Cbp, Brochure *Gedragscodes Bescherming van persoonsgegevens door zelfregulering*, Oktober 2002.

Cbp Informatieblad
Cbp, Informatieblad, *Informatieplicht*, nummer 14A, februari 2007.

Cbp Richtsnoeren Persoonsgegevens op internet
Cbp, *Richtsnoeren Publicatie van persoonsgegevens op internet*, december 2007.

Cbp Wetgevingsadvies
Wetgevingsadvies CBP inzake wijziging van de Telecommunicatiewet, 4 juni 2010, z2010-00475.

The Center for Information Policy Leadership 2007
The Center for Information Policy Leadership at Hunton & Williams LLP, *Ten steps to develop a multilayered privacy notice*, Prepared by leading lawyers and experts in privacy with The Center for Information Policy Leadership, 2007.

The Center for Information Policy Leadership 2009
The Center for Information Policy Leadership at Hunton & Williams LLP, *Data Protection Accountability: The Essential Elements. A Document for Discussion,* Prepared by the Centre for Information Policy Leadership as Secretariat to the Galway Project, 2009.

The Center for Information Policy Leadership 2010
The Center for Information Policy Leadership at Hunton & Williams LLP, *Demonstrating and Measuring Accountability A Discussion Document. Accountability Phase II – The Paris Project*, Prepared by the Centre for Information Policy Leadershipas Secretariat to the Paris Project, 2010.

Ciocchetti
C.A. Ciocchetti, 'The Future of Privacy Policies: A Privacy Nutrition Label Filled With Fair Information Practices', Selected Works of Corey A. Ciocchetti, 2009.

COM (2003) 265 definitief
Commissie van de Europese Gemeenschappen, Verslag van de Commissie, Eerste verslag over de toepassing van de Richtlijn gegevensbescherming (95/46/EG), Brussel, 15.5.2003, COM (2003) 265 definitief.

COM (2010) 609 definitief
Commissie van de Europese Gemeenschappen, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie, Brussel, 4.11.2010, COM (2010) 609 definitief.

COM (2012) 9 final
European Commission, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century, Brussel, 25.1.2012, COM (2012) 9 final.

COM (2012) 11 final
European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussel, 25.1.2012, COM (2012) 11 final.

Cuijpers 2004
C.M.K.C. Cuijpers, *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn* (diss. Tilburg), Wolf Legal Publishers (WLP) 2004.

Cuijpers 2007
C. Cuijpers, 'A Private Law Approach to Privacy; Mandatory Law Obliged?', *Scripted*, Volume 4, Issue 4, September 2007, p. 304-318.

Cuijpers et al.
C. Cuijpers, R. Leenes, S. Olislaegers & K. Stuurman, *De wolk in het onderwijs. Privacy aspecten bij cloud computing services*, Tilburg Institute for Law, Technology, and Society (TILT), 2011.

Department of Commerce
Department of Commerce, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, the department of commerce internet policy task force, December 2010.

Van Dijck
G. van Dijck, 'Empirical Legal Studies (ELS)', *WPNR (*6912) 2011, p. 1105-1112.

McDonald
A.M. McDonald, *Footprints Near the Surf: Individual Privacy Decisions in Online Contexts* (diss. Pittsburgh, Verenigde Staten), Carnegie Mellon University, 2010.

McDonald et al.
A.M. McDonald, R.W. Reeder, P.G. Kelly & L.F. Cranor, 'A Comparative Study of Online Privacy Policies and Formats', authors pre-press version, 2009, te verkrijgen via www.springer.de/comp/lncs/index.html.

McDonald & Cranor
A.M. Mcdonald & L.F. Cranor, 'The Cost of Reading Privacy Policies', *ACM Transactions on Computer-Human Interaction*, 4(3), 2008, p. 1-22.

Dommering 2000
E.J. Dommering e.a., *Informatierecht. Fundamentele rechten voor de informatiesamenleving*, Amsterdam: Otto Cramwinckel Uitgever 2000.

Dommering 2007
E.J. Dommering, annotatie bij twee arresten van de Hoge Raad 29 juni 2007 (*Dexia* en *HBU*), *NJ* 2007-51, nr. 639.

Dommering 2010
E.J. Dommering, 'Recht op persoonsgegevens als zelfbeschikkingsrecht', in: C. Prins, Q. Eijkman, L. Egmond, V. Böhre & M. Heerings, *16 Miljoen BN'ers. Bescherming van Persoonsgegevens in het Digitale Tijdperk*, Leiden: Stichting NJCM-Boekerij 2010, p. 83-98.

Van Driel
M. van Driel, *Zelfregulering. Hoog opspelen of thuisblijven*, (diss UvU), Deventer: Kluwer 1989.

Dubbeld
L. Dubbeld, 'Privacybeleid van Nederlandse telemedicine websites', *Privacy & Informatie* 2006, afl. 3, p. 132 -136.

Duthler
A.W. Duthler, 'Kabinetsplannen voor toekomst privacybescherming', *P&I* 2010-2, 50, p. 59-64.

Earp et al.
J.B. Earp, A.I. Antón, L. Aiman-Smith & W.H. Stufflebeam, 'Examining Internet Privacy Policies Within the Context of User Privacy Values', *IEEE Transactions on Engineering Management*, Vol. 52, No. 2, May 2005, p. 227-237.

EDPS
European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"*, Brussels, 14 January 2011.

Van Esch & Blok
R. van Esch & P. Blok, 'Privacy en elektronische handel via internet', in: J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2007, p. 203-226.

Essers
P.H.J. Essers, 'Codificatie en dynamiek in het belastingrecht, in: J.B.M. Vranken & I. Giesen, *Codificatie en dynamiek. Instrumenten ter begeleiding van de omgang van codificaties*, Schoordijk Instituut, Den Haag: Boom Juridische uitgevers 2004, p. 7-27.

Eijlander 1993
Ph. Eijlander, *De wet stellen. Beschouwingen over onderwerpen van wetgeving*, Zwolle: W.E.J. Tjeenk Willink 1993.

Eijlander 1994
Ph. Eijlander, 'Zelfregulering in soorten en maten' in: Ph. Eijlander, P.H.A. Frissen, e.a., *Wetgeven en de maat van tijd*, Zwolle: W.E.J. Tjeenk Willink 1994, p. 93-104.

Eijlander & Voermans
Ph. Eijlander & W.J.M. Voermans, *Wetgevingsleer*, Deventer: W.E.J. Tjeenk Willink 1999.

Federal Trade Commission
Federal Trade Commission, *Protecting Consumer Privacy in a Era of Rapid Change. A proposed framework for business and policymakers*, Preliminary FTC Staff Report, December 2010.

Flash Eurobarometer
European Commission, *Attitudes towards crossborder sales and consumer protection. Analytical report*, Flash Eurobarometer 282, The Gallup Organization, March 2010.

Geelhoed
L.A. Geelhoed, 'Deregulering, herregulering en zelfregulering' in: Ph. Eijlander, P.C. Gilhuis & J.A.F. Peters, *Overheid en zelfregulering. Alibi voor vrijblijvendheid of prikkel tot aktie?*, Zwolle: W.E.J. Tjeenk Willink 1993, p. 33-51.

Giesen 2007-a
I. Giesen, Alternatieve regelgeving in privaatrechtelijke verhoudingen, in: Witteveen, Giesen & De Wijkerslooth, *Alternatieve regelgeving, Preadviezen*, Handelingen Nederlandse Juristen-Vereniging, p. 67-152, Deventer: Kluwer 2007.

Giesen 2007-b
I. Giesen, *Alternatieve regelgeving en privaatrecht*, Monografieën Privaatrecht, Deventer: Kluwer 2007.

Groenhuijsen
M.S. Groenhuijsen, 'Uitvoeringsmaatregelen', in: J.B.M. Vranken & I. Giesen, *Codificatie en dynamiek. Instrumenten ter begeleiding van de omgang van codificaties*, Schoordijk Instituut, Den Haag: Boom Juridische uitgevers 2004, p. 201-206.

Groep Gegevensbescherming Artikel 29-2000
Groep Gegevensbescherming Artikel 29, Werkdocument *Privacy op internet - Een geïntegreerde EU-aanpak van on-linegegevensbescherming*, goedgekeurd op 21 november 2000, WP 37, 5063/00/NL/DEF.

Groep Gegevensbescherming Artikel 29-2001
Groep Gegevensbescherming Artikel 29, *Aanbeveling inzake bepaalde minimumeisen voor het on line verzamelen van persoonsgegevens in de Europese Unie*, goedgekeurd op 17 mei 2001, WP 43, 5020/01/NL/def.

Groep Gegevensbescherming Artikel 29-2004
Groep Gegevensbescherming Artikel 29, Advies 10/2004 over meer geharmoniseerde bepalingen inzake informatieverstrekking, goedgekeurd op 25 november 2004, WP 100, 11987/04/NL.

Groep Gegevensbescherming Artikel 29-2009
Article 29 Data Protection Working Party & Working Party on Police and Justice, *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, adopted on 01 December 2009, WP 168, 02356/09/EN.

Groep Gegevensbescherming Artikel 29-2010 (I)
Groep Gegevensbescherming Artikel 29, *Advies 2/2010 over online reclame op basis van surfgedrag ('behavioural advertising')*, goedgekeurd op 22 juni 2010, WP 171, 00909/10/NL.

Groep Gegevensbescherming Artikel 29-2010 (II)
Groep Gegevensbescherming Artikel 29, *Advies 3/2010 over het verantwoordingsbeginsel*, goedgekeurd op 13 juli 2010, WP 173, 00062/10/NL.

Groep Gegevensbescherming Artikel 29-2011
Groep Gegevensbescherming Artikel 29, *Opinion 15/2011 on the definition of consent*, adopted on 13 July 2011, WP 187, 01197/11/EN.

De Hert 2009
P. de Hert, *In het licht van de technologie. Pleidooi voor continuïteit en verandering bij gegevensbescherming*, Den Haag: College bescherming persoonsgegevens / Universiteit van Tilburg 2009.

De Hert 2011
P. de Hert, Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechtenverplichting, in: D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.), *De staat van informatie*, Amsterdam: Amsterdam University Press 2011.

Hijma & Olthof
Prof. mr Jac. Hijma & mr M.M. Olthof, *Compendium van het Nederlands vermogensrecht*, Negende druk, Deventer: Kluwer 2005.

Hildebrandt
M. Hildebrandt, 'Privacy en identiteit in slimme omgevingen', *Computerrecht* 2010-6, p. 273-282.

Hochhauser
M. Hochhauser, *Why Patients Won't Understand Their HIPAA Notices*, Privacy Rights Clearinghouse, 2003.

Holleman 2003
A. Holleman, 'Privacystatements op het internet' *Privacy & Informatie* 2003, afl. 6, p. 253-258.

Holleman 2005
A. Holleman, 'Verantwoordelijk voor verenigbaar gebruik ex artikel 9 Wbp', *Privacy & Informatie* 2005, afl. 4, p. 164-168.

Holvast
J. Holvast, 'Interview met Jacob Kohnstamm', *P&I* 2005-3, p. 114-119.

Holvast & Gardeniers
J. Holvast & H. Gardeniers, *Privacy, zelfregulering en Internet*, Eindrapport, Mei 2001.

Hooghiemstra & Nouwt
Th. Hooghiemstra & S. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: Sdu 2007.

Hoving
E. Hoving, 'De privacyverklaring als overeenkomst: een brug te ver?', *Privacy & Informatie* 2009, afl. 3, p. 127-131.

Jensen & Potts 2003
C. Jensen & C. Potts, 'Privacy Policies Examined: Fair Warning or Fair Game?', *GVU* Technical Report 03-04 (Feb. 2003).

Jensen & Potts 2004
C. Jensen & C. Potts, 'Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices', *CHI* 2004, vol. 6, p.471-478 (2004).

Jones & Tahri
R. Jones & D. Tahri, 'EU law requirements to provide Information to website visitors', Computer Law & Security Review 26 (2010), p. 613-620.

Jongeneel
R.H.C. Jongeneel, 'Werkingssfeer afdeling 6.5.3', in: B. Wessels, R.H.C. Jongeneel & M.L. Hendrikse, *Algemene Voorwaarden*, Deventer: Kluwer 2006, p.90-96.

Kelly et al. 2008
P.G. Kelly, S.S. Won & L.F. Cranor, '*Design of a Privacy Label for P3P Policies*, Carnegie Mellon University, 2008.

Kelly et al. 2009
P.G. Kelly, J. Breese, L.F. Cranor & R.W. Reeder, 'A "Nutrition Label" for Privacy', in *Proceedings of the 2009 Symposium On Usable Privacy and Security (SOUPS)*, 2009.

Kelly et al. 2010
P.G. Kelly, J. Breese, L.F. Cranor & R.W. Reeder, 'Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach', *Technical Report CMU-CyLab*-09-014, Carnegie Mellon University, January 12, 2010.

Van der Klaauw-Koops
F.A.M. van der Klaauw-Koops, 'Het totstandkomen van elektronische contracten', in: R.E. van Esch (red.), J.E.J. Prins (red.) e.a., *Recht en elektronische handel*, tweede druk, Deventer: Kluwer 2002, p. 127-143.

Kleen & Heinrichs
B.A. Kleen & L.R. Heinrichs, 'Are privacy policies more clear and conspicous in 2006 than 2001? A longitudinal study of het Fortune 100', *Issues in Information Systems*, Volume VIII, No. 2, 2007, p. 348-354.

Kleimann 2006
Kleimann Communication Group, Inc, *Evolution of a Prototype Financial Privacy Notice. A report on the Form Development Project*, February 28, 2006.

Kleimann 2009
Kleimann Communication Group, Inc, Web-based Financial Privacy Notice Final Summary Findings Report, Presented to U.S. Federal Trade Commission, October 29, 2009.

Koops
B.J. Koops, 'The Evolution of Privacy Law and Policy in the Netherlands', *Journal of Comparative Policy Analysis*, Vol. 13, No. 2, April 2011,p. 165-179.

Koops et al.
B.J. Koops, M. Lips, S. Nouwt, C. Prins & M. Schellekens, 'Should self-regualtion be the starting point?', in: B.J. Koops, M. Lips, C. Prins en M. Schellekens, *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, Information Technology & Law Series, The Hague: TMC Asser press 2006, p. 109-149.

Van Laarhoven
M.J. van Laarhoven, *Samenhang in rechtsverhoudingen* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2006.

Levy & Hastak
A. Levy & M. Hastak, *Consumer Comprehension of Financial Privacy Notices. A Report on the Results of the Quantitative Testing*, submitted to Interagency Notice Project, December 15, 2008.

Lindahl
H.K. Lindahl, 'Zelfregulering: rechtsvorming, democratie en reflexieve identiteit', *Rechtsgeleerd Magazijn THEMIS*, 2006- 2, p. 39-48.

Lindenbergh
S.D. Lindenbergh, *Smartengeld, tien jaar later*, Deventer: Kluwer 2008.

Luijendijk & Senden
H. Luijendijk & L.A.J. Senden, 'De gelaagde doorwerking van Europese administratieve soft law in de nationale rechtsorde', NVER preadviezen, 2011.

Maritius
H.P.A.K. Maritius, 'Algemene voorwaarden en E-commerce' in: B. Wessels, R.H.C. Jongeneel & M.L. Hendrikse, *Algemene Voorwaarden*, Deventer: Kluwer 2006, p. 379-408.

Meinert et al
D.B. Meinert, D.K. Peterson, J.R. Criswell & M.D. Crossland, 'Would Regulation of Web Site Privacy Policy Statements Increase Consumer Trust?', *Informing Science Journal*, Volume 9, 2006, p. 123-142.

Milne & Culnan
G.R. Milne & M.J. Culnan, 'Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices', *Journal of Interactive Marketing*, volume 18, number 3, summer 2004, p. 15-29.

Moerel
E.M.L. Moerel, *Binding Corporate Rules, Fixing the Regulatory Patchwork of Data Protection* (diss. Tilburg), Amsterdam: Moerel 2011.

NGFG
Het Nederlands Genootschap van Functionarissen voor de gegevensbescherming (NGFG), *Response to : Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union COM(2010) 609 final*, January 15th 2011.

Nota Wes
Nota Wetgeving voor de elektronische snelweg, Kamerstukken II, vergaderjaar 1997 – 1998, 25880, nrs. 1 – 2.

Nouwt 2005
S. Nouwt, *Privacy voor doe-het-zelvers*, Nationaal Programma Informatietechnologie en Recht (IteR) 73, Den Haag: Sdu Uitgevers 2005.

Nouwt 2009
S. Nouwt, 'Towards a Common European Approach to Data Protection: A Critical Analysis of Data Perspectives of the Council of Europe and the European Union', in: S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwange & S. Nouwt, *Reinventing Data Protection?*, Dordrecht: Springer 2009, p. 275-292.

OECD
Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980.

Oussayef
K.Z. Oussayef, 'Selective Privacy: Facilitating Market-Based Solutions to Data Breaches by Standardizing Internet Privacy Policies', *B.U. J. SCI. & TECH. L.,* Vol. 14, 2008, p. 104-131.

Overkleeft-Verburg
G. Overkleeft-Verburg, *De Wet Persoonsregistraties. Norm, toepassing en evaluatie* (diss. Tilburg), Katholieke Universiteit Brabant, 1995.

Pan & Zinkhan
Y. Pan & G.M. Zinkhan, 'Exploring the impact of online privacy disclosures on consumer trust', *Journal of Retailing*, Volume 82, Issue 4, 2006, p. 331-338.

Papacharissi & Fernback
Z. Papacharissi & J. Fernback, 'Online Privacy and Consumer Protection: An Analysis of Portal Privacy Statements', *Journal of Broadcasting & Electronic Media* 49(3), 2005, p. 259-281.

Pedersen
A. Pedersen, 'Taking the confusion out of privacy notices', *Privacy Laws & Business International Newsletter*, October/November 2003, p. 31-33.

Peng et al.
H. Peng, J. Gu & X. Ye, 'Towards Compliance and Accountability: a Framework for Privacy Online', *Journal of Computers*, Vol. 4, No. 6, June 2009, p. 494-501.

Privacy notices code of practice
Information Commissioner's Office, *Privacy notices code of practice*, June 2009.

Prins 2010
J.E.J. Prins, 'Burgers en hun privacy: over verhouding en houding tot een ongemakkelijk bezit', in: C. Prins, Q. Eijkman, L. Egmond, V. Böhre & M. Heerings, *16 Miljoen BN'ers. Bescherming van Persoonsgegevens in het Digitale Tijdperk*, Leiden: Stichting NJCM-Boekerij 2010, p. 1-13.

Prins 2011
J.E.J. Prins, 'De eOverheid voorbij. Recht doen aan de digitale werkelijkheid', in Groothuis, Prins & Schuyt, *De digitale overheid, Preadviezen*, VAR-reeks 146, p. 71-114, Den Haag: Boom Juridische uitgevers 2011.

Prins et al.
J.E.J. Prins, W.B.H.J. van de Donk, H.P.M. van Duivenboden, K. ten Have, J. Nouwt, H.A.C.M. Vorselaars & S. Zouridis, *In het licht van de Wet persoonsregistraties: zon, maan of ster?*, Nationaal Programma Informatietechnologie en Recht (ITeR) 1, Alphen aan den Rijn/Diegem: Samson Bedrijfsinformatie 1995.

Proctor et al.
R.W. Proctor, M. Athar Ali & K-P.L. Vu, 'Examining Usablilty of Web Privacy Policies', *International Journal of Human-Computer Interaction*, 24(3), 307-328, 2008.

Purtova
N. N. Purtova, *Property Rights in Personal Data: a European Perspective* (diss. Tilburg), Oisterwijk: Uitgeverij BOXPress 2011.

Raab
Ch.D. Raab, *The future of privacy protection*, Cyber Trust & Crime Prevention Project, Edinburgh University, 2004.

Raad van Europa
Council of Europe, Modernisation of Convention 108: proposals, Bureau of the Consultative Committtee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), T-PD-BUR(2011) 19_en, Strasbourg, 3 October 2011.

Regioplan
Regioplan Beleidsonderzoek, *Niets te verbergen en toch bang. Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving*, Regioplan publicatienr. 1774, Amsterdam, januari 2009.

Registratiekamer
Registratiekamer, *Klant in het web. Privacywaarborgen voor internettoegang*, Achtergrondstudies en Verkenningen, nummer 17.

Rodrigues
P. Rodrigues, 'Vraagbaak privacy en algemene voorwaarden', *P&I* 2000, afl. 1, p. 45-46.

Roosendaal
A. Roosendaal, 'Facebook tracks and traces everyone: Like this!', *SSRN* 2011, 1717563.

Schreuders
E. Schreuders, *Toestemming of ondubbelzinnige toestemming?*, 16 juni 2011, te downloaden via http://privacydossier.weebly.com.

Senden
L.A.J. Senden, *Soft law in European Community Law:Its relationship to legislation* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2003.

Siemerink
L.A.R. Siemerink, *De overeenkomst van Internet Service Providers met consumenten* (diss. Leiden), Deventer: Kluwer 2007.

Siemerink et al.
L.A.R. Siemerink, M. van Eijden & R.E. van Esch, 'Uitsluiting of beperking van aansprakelijkheid via disclaimers op een website', *Computerrecht* 2006-3, p. 143-149.

Van der Sloot 2010
B. van der Sloot, 'De privacyverklaring als onderdeel van een wederkerige overeenkomst', *Privacy & Informatie* 2010, afl. 3, p. 106-109.

Van der Sloot 2011-a
B. van der Sloot, 'Je geld of je gegevens', *NJ* 2011, afl. 23, p. 1493-1496.

Van der Sloot 2011-b
B. van der Sloot, 'De evaluatie van de Wet bescherming persoonsgegevens', *Privacy & Informatie* 2011, afl. 5, p. 224-236.

Stuurman
C. Stuurman, 'Ambient intelligence: een heerlijke nachtmerrie?', *Computerrecht* 2010-6, p. 262-266.

Tempelman
J.A. Tempelman, 'De richtlijn Privacy en elektronische communicatie', *Privacy & Informatie* 2003, afl. 5, p. 196-205.

Teunissen
J.M.H.F. Teunissen, *Alternatieve regelgeving en eigen verantwoordelijkheid* (oratie Heerlen), Nijmegen: Wolf Legal Publishers 2007.

Thijssen
M.B.J. Thijssen, *De Wbp en de vennootschap* (diss. Nijmegen), Deventer: Kluwer 2009.

Thuiswinkel Markt Monitor
Thuiswinkel Markt Monitor, *Online verkopen t/m december 2009*, B11345, Blauw Research bv, April 2010.

Thuiswinkel Markt Monitor Brancherapport segment Verzekeringen
Thuiswinkel Markt Monitor, *Brancherapport segment Verzekeringen Online verkopen t/m december 2009*, B11346, Blauw Research bv, Juni 2010.

TNO/IViR
TNO & IViR, *A bite too big: Dilemma's bij de implementatie van de Cookiewet in Nederland*, TNO-rapport, 28 februari 2011, nr. 35473.

TNS NIPO
TNS NIPO Consult, De naleving en beleving van de informatieplicht onder organisaties in Nederland, Onderzoek onder huisartsen, onderwijsinstellingen en woningcorporaties, Z1684, Februari 2006.

Turow
J. Turow, *Americans & Online Privacy. The System is Broken*, A Report from the Annenberg Public Policy Center of the University of Pennsylvania, 2003.

Vail et al.
M.W. Vail, J.B. Earp & A.I. Antón, 'An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies', *IDEEE Transactions on Engineering Management*, Vol. 55, No. 3, August 2008, p. 442-454.

Verburg
G.J.M. Verburg, *Vaststelling van smartengeld* (diss. Leiden), Deventer: Kluwer 2009.

Verkade
D.W. Verkade, noot bij HR 29 juni 2007 (*Dexia*), *NJ* 2007, 638.

Versmissen
K. Versmissen, 'Privacy Compliance – Een tour d'horizon', *Privacy & Compliance*, 2011-1, p. 6-12.

Vranken 2004-a
J.B.M. Vranken, 'Niets in het recht is blijvend, behalve verandering', *WPNR* (6560) 2004, p. 1-13.

Vranken 2004-b
J.B.M. Vranken, 'Codificatie en dynamiek in het burgerlijk procesrecht. Begeleidingsinstrumenten bij de hantering van een (her)codificatie', in: J.B.M. Vranken & I. Giesen, *Codificatie en dynamiek. Instrumenten ter begeleiding van de omgang van codificaties*, Schoordijk Instituut, Den Haag: Boom Juridische uitgevers 2004, p. 51-64.

Vranken 2011
J.B.M. Vranken, 'Een nieuw rechtsrealisme in het privaatrecht', *WPNR (*6912) 2011, p. 1113-1122.

Vranken & Van Dijck
J.B.M. Vranken & G. van Dijck, 'Law and ... bewegingen: Een slotbeschouwing', *WPNR (*6912) 2011, p. 1123-1127.

De Vries 2009
H.H. de Vries, *Tekst & Commentaar Telecommunicatierecht*, Deventer: Kluwer 2009.

De Vries 2011
H.H. de Vries, 'Netneutraliteit & cookies: Nederland als Europese safe haven?', *Computerrecht* 2011/4, 96, p. 183-185.

Vu, Chambers, Garcia et al.
K.P.L. Vu, V. Chambers, F.P. Garcia, B. Creekmur, J. Sulaitis, D. Nelson, Russell Pierce & R.W. Proctor, 'How Users Read and Comprehend Privacy Policies', in: M.J. Smith, G. Salvendy (Eds.), *Human Interface*, Part II, HCII 2007, LNCS 4558, p. 802-811, 2007.

Vu, Garcia, Nelson et al.
K.P.L. Vu, F.P. Garcia, D. Nelson, J. Sulaitis, B. Creekmur, V. Chambers & R.W. Proctor, 'Examining User Privacy Practices While Shopping Online: What Are Users Looking for?', in: M.J. Smith, G. Salvendy (Eds.), *Human Interface*, Part II, HCII 2007, LNCS 4558, p. 792-801, 2007.

Van Wechem
T.H.M. van Wechem, *Toepasselijkheid van algemene voorwaarden*, Deventer: Kluwer 2007.

Wagemans
A.W. Wagemans, 'Zelfreguleringsinitiatieven', in: R.E. van Esch & J.E.J. Prins, *Recht en elektronische handel*, Deventer: Kluwer 2002, p. 61-85.

Wessels, Jongeneel en Hendrikse
B. Wessels, R.H.C. Jongeneel & M.L. Hendrikse, *Algemene Voorwaarden*, Deventer: Kluwer 2006.

Winter et al.
H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A.M. Klingenberg & H. Prakken, *Wat niet weet, wat niet deert, een evaluatie naar de werking van de Wet bescherming persoonsgegevens in de praktijk*. Dit rapport is uitgebracht in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) te Den Haag en is geschreven door een onderzoeksteam van Pro Facto RuG en de Vakgroep Bestuursrecht en Bestuurskunde van de RuG. Groningen, september 2008.

Witteveen
W.J. Witteveen, 'Alternatieve regulering: de vele gezichten van de wetgever', in: Witteveen, Giesen & De Wijkerslooth, *Alternatieve regelgeving, Preadviezen*, Handelingen Nederlandse Juristen-Vereniging, p.3-65, Deventer: Kluwer 2007.

WRR rapport *i*Overheid
Wetenschappelijke Raad voor het Regeringsbeleid, *iOverheid*, Amsterdam: Amsterdam University Press 2011.

Van der Zee
F. van der Zee, *Kennisverwerving in de Empirische Wetenschappen. De methodologie van wetenschappelijk onderzoek*, Groningen: BMOOO 2007.

Zuiderveen Borgesius
F.J. Zuiderveen Borgesius, 'De meldplicht voor datalekken in de Telecommunicatiewet', *Computerrecht* 2011/4, 99, p. 209-218.

Zwenne et al.
G-J. Zwenne, A-W. Duthler, M. Groothuis, H. Kielman, W. Koelewijn & L. Mommers, *Eerste fase evaluatie Wet bescherming persoonsgegevens, Literatuuronderzoek en knelpuntenanalyse*. WODC / Ministerie van Justitie 2007, december 2007.